American Business Law Journal

American Business Law Journal
Volume 51, Issue 4, 779–841, Winter 2014

Employee Internet Privacy: A Proposed Act that Balances Legitimate Employer Rights and Employee Privacy

*Susan Park**

INTRODUCTION

When Justin Basset interviewed for a job in New York City in 2012, he expected to respond to questions one is typically asked in a job interview. However, his interview took a modern technological twist when the interviewer opened her computer and attempted to look at Mr. Basset's Facebook profile on her computer. Unable to see the details of his profile because he had taken advantage of Facebook's privacy options to limit public viewing, she asked for his login information to access his account. He declined and withdrew his application.[1] In 2010, Robert Collins, a Maryland Department of Public Safety and Correctional Services employee, was interviewed to determine whether he was eligible for reinstatement after taking a leave of absence following a death in the family. His supervisors asked for his Facebook password during the interview so they could look at his profile to help them determine whether he was

*J.D., Assistant Professor of Legal Studies in Business, Boise State University. This work was generously supported through a summer research grant from the Boise State University College of Business and Economics. The author thanks Boise State MBA Graduate Assistant Molly Haberl for her valuable research and analysis and W. Anthony Park and Betsy Hall for their editorial suggestions.

[1]Manuel Valdes & Shannon McFarland, *Employers Ask Job Seekers for Facebook Passwords*, SEATTLE TIMES (Mar. 20, 2012, 4:36 AM), http://seattletimes.com/html/nationworld/2017794577_apusjobapplicantsfacebook.html.

involved in gang-related activity. He complied, reluctantly.[2] In 2009, the City of Bozeman, Montana, employed a practice of asking job applicants for password information for their e-mail, social networking, and other online accounts.[3] Similar incidents in Illinois, Virginia, and Michigan have also been reported.[4]

The number of employers who search the Internet for information about job applicants and employees has been on the rise for years. This phenomenon has been widely reported and is almost universally considered to be legally permissible.[5] However, this avenue for information gathering may be becoming less fruitful for employers as more social media users adjust their privacy settings to restrict access to their profiles.[6]

---

[2]Allie Bohm, *Maryland Legislature to Employers: Hands Off Facebook Passwords*, ACLU Blog of Rights (Apr. 9, 2012), http://www.aclu.org/blog/technology-and-liberty/maryland-legislature-employers-hands-facebook-passwords (quoting Collins, "I felt violated, I felt disrespected, I felt that my privacy was invaded. But not only my privacy, the privacy of my friends and that of my family that didn't ask for that."); *see also* Robin M. Sheridan, *New Password Protection Laws Have Employers A-"Twitter"*, HR Insights for Health Care (Oct. 30, 2012), http://www.hallrender.com/insights/new-password-protection-laws-have-employers-a-twitter.

[3]Valdes & McFarland, *supra* note 1; *see also* Matt Gouras, *Montana City Asks Job Applicants for Facebook Passwords*, Huffington Post (June 19, 2009, 8:58 PM), http://www.huffingtonpost.com/2009/06/19/montana-ckty-asks-job-app_n_218152.html; Declan McCullagh, *Want a Job? Give Bozeman Your Facebook, Google Passwords*, CNET News (June 18, 2009, 4:52 PM), http://news.cnet.com/8301-13578_3-10268282-38.html.

[4]Valdes & McFarland, *supra* note 1; *see also* Megan Garber, *Is Your Facebook Password Like Your Mail, House Key, or Drug Test?*, Atlantic (Apr. 3, 2012, 7:19 AM), http://www.theatlantic.com/technology/archive/2012/04/is-your-facebook-password-like-your-mail-house-key-or-drug-test/255354/ (reporting on an incident occurring in Michigan).

[5]*See, e.g.*, Robert Sprague, *Rethinking Information Privacy in an Age of Online Transparency*, 25 Hofstra Lab. & Emp. L.J. 395, 401 (2008) ("The manner in which the right to privacy in the United States has developed. . . affords essentially no protection for applicants when prospective employers turn to the Internet to investigate their thoughts, musings, recreations, or even what others may have said about them online."); *Managing Your Online Image Across Social Networks*, Reppler Effect (Sept. 27, 2011), http://blog.reppler.com/2011/09/27/managing-your-online-image-across-social-networks/ (reporting that a Reppler survey of three hundred professionals involved in their companies' hiring process revealed that ninety-one percent use social networking to screen job applicants).

[6]*See* Mary Madden, Privacy Management on Social Media Sites 7–8, 13 (2012), *available at* http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf (reporting that a 2011 national survey of 2277 adults revealed that fifty-eight percent restrict access to their social media profiles); Benny Evangelista, *Facebook Friend Lists Shrinking to Guard Privacy*, SFGate (Feb. 25, 2012), http://www.sfgate.com/business/article/Facebook-friend-lists-shrinking-to-guard-privacy-3360189.php;

Thus, at least some employers have begun to ask for social media username or password information so they can take a look behind the scenes to learn more about the applicant or employee.[7] Facebook and others who follow developments in social media have expressed alarm at what they believe is a growing trend that has important privacy implications.[8] Others argue that these incidents are isolated and are not indicative of a meaningful shift in employer behavior.[9]

Alexia Tsotsis, *Most People Have Changed Their Privacy Settings on Facebook, Says Facebook CTO*, TECHCRUNCH (Oct. 19, 2011), http://techcrunch.com/2011/10/19/most-people-have-changed-their-privacy-settings-on-facebook-says-facebook-cto/ (quoting Facebook CTO Bret Taylor that "the majority of people on Facebook have modified their privacy settings"); *What Is the "Norm" for Privacy Settings on Social Networking Sites?*, IKEEPSAFE, http://www.ikeepsafe.org/be-a-pro/privacy/what-is-the-norm-for-privacy-settings-on-social-networking-sites/ ("That 80% of the public goes to the effort of changing their settings to private indicates that users care deeply about their privacy online . . . .").

[7]*See supra* text accompanying notes 1–4; *see also* Jerilyn Jacobs, *What's Your Password? Pending Password Protection Provisions*, GONZALEZ SAGGIO & HARLAN (Aug. 29, 2012), http://www.gshllp.com/60-second-memos/whats-your-password-pending-password-protection-provisions (stating that as job applicants "began limiting what information from their accounts was available to the public, some employers decided to raise the stakes even higher by asking applicants to provide their user name [and] passwords so that the employer could access the site and take a look around").

[8]*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, 511 (2013) ("[T]here is a disturbing emergence of reports of demands by public and private employers and academic institutions for access to users' private social media account content."); Chloe Albanesius, *Maryland OKs Bill Banning Employers from Requesting Passwords*, PC MAG. (Apr. 10, 2012), http://www.pcmag.com/article2/0,2817,2402852,00.asp (noting reports emerging "of employers asking current and prospective employees to hand over passwords or access to services like Facebook"); Erin Egan, *Protecting Your Passwords and Your Privacy*, FACEBOOK (Mar. 23, 2012, 5:32 AM), https://www.facebook.com/note.php?note_id=326598317390057 ("In recent months, we've seen a distressing increase in reports of employers or others seeking to gain inappropriate access to people's Facebook profiles or private information."); Zach Walton, *SNOPA Is One Internet Bill Worth Rooting For*, WEBPRONEWS (Apr. 27, 2012), http://www.webpronews.com/snopa-is-one-internet-bill-worth-rooting-for-2012-04 ("[I]t bears repeating just how bad of a problem this is. In short, it turns out that there's a disturbing trend among American employers asking for applicants' Facebook passwords.").

[9]*See, e.g.*, Eric Gaydos, *Relax—You'll Never, Ever Be Asked for a Facebook Password*, TLNT (May 15, 2012, 8:35 AM), http://www.tlnt.com/2012/05/15/relax-youll-never-ever-be-asked-for-a-facebook-password/; Philip L. Gordon, *Illinois' New Social Media Password Law Raises Substantial and Unjustified Obstacles to Employers' Legitimate Business Activities*, WORKPLACE PRIVACY COUNS. (May 29, 2012), http://www.littler.com/2012/05/articles/state-privacy-laws/illinois-new-social-media-password-law-raises-substantial-and-unjustified-obstacles-to-emplo ("Despite the absence of a proven need, the Illinois bill imposes apparently broad restrictions on

Trend or not, state legislatures have taken notice. After the Robert Collins incident in Maryland caught the attention of the media and the American Civil Liberties Union (ACLU) (which convinced the Department of Corrections to stop the practice),[10] the Maryland General Assembly took action and, in 2012, became the first state to enact legislation that prohibits employers from asking for social media login information.[11] Since then, sixteen more states have passed similar statutes,[12] while twenty-seven others have considered comparable legislation.[13] Congress too has joined the movement,

---

employers."); Jon Hyman, *Ohio Joins the Fray on Employers Asking for Social Media Passwords*, Ohio Employer's Law Blog (May 29, 2012), http://www.ohioemployerlawblog.com/2012/05/ohio-joins-fray-on-employers-asking-for.html (asserting that companies are not engaging in the type of conduct the Ohio social media password bill seeks to legislate); Elizabeth Torphy-Donzella, *Maryland Password Protection Law Takes Effect*, Lab. & Emp. Rep. (Oct. 10, 2012), http://www.laboremploymentreport.com/2012/10/10/maryland-password-protection-law-takes-effect/ ("[W]hat is not apparent is that this is a widespread problem that required legislative action.").

[10]Ateqah Khaki, *Status Update: Employers Asking for Your Facebook Password Violates Your Privacy and the Privacy of All Your Friends, Too*, ACLU Blog of Rights (Mar. 22, 2012, 2:49 PM), https://www.aclu.org/blog/technology-and-liberty/status-update-employers-asking-your-facebook-password-violates-your ("As soon as his job interview at the Department of Corrections ended, Collins contacted the ACLU of Maryland (on his way to the car, in fact!) and soon after, Legal Director Deborah Jeon wrote a letter to the department. . . . A few months later, the department reconsidered its policy, and instead began asking applicants to 'voluntarily' provide access to their accounts during interviews.").

[11]Md. Code Ann., Lab. & Empl. § 3-712 (West 2012).

[12]Ark. Code Ann. § 11-2-124 (West 2013); Cal. Lab. Code § 980 (West 2013); Colo. Rev. Stat. Ann. § 8-2-127 (West 2013); 820 Ill. Comp. Stat. Ann. 55/10 (West 2012); 2014 La. Act 165 (to be codified at La. Rev. Stat. Ann. 51:1951–1955 (2014)); Mich. Comp. Laws Ann. §§ 37.271–278 (West 2012); Nev. Rev. Stat. Ann. § 613.135 (West 2013); N.J. Stat. Ann. §§ 34:6B-5–10 (West 2013); N.M. Stat. Ann. § 50-4-34 (West 2013); H.B. 2372, Reg. Sess. (Okla. 2014) (to be codified at Okla. Stat. Ann. tit. 40, §§ 173.2, 173.3 (West 2014)) (effective Nov. 1, 2014); Or. Rev. Stat. § 659A.330 (West 2014); 2014 R.I. Pub. Law S2095A (to be codified at R.I. Gen. Laws Ann. § 28-56-1–6 (West 2014) (effective June 30, 2014); Tenn. Pub. Act No. 2014-826 (effective Jan. 1, 2015); Utah Code Ann. §§ 34-48-101–301 (West 2013); Wash. Rev. Code Ann. §§ 49.44.200, 205 (West 2013); Wis. Stat. Ann. § 995.55 (West 2014). As of the time this article went to press, New Hampshire's legislature had passed a bill prohibiting employers from requesting access to employees' and prospective employees' personal accounts, but it had not yet been signed by the governor. *See* H.B. 1407, 2014 Leg., Reg. Sess. (N.H. 2014).

[13]In 2012, according to the National Conference of State Legislatures (NCSL), the following states considered but did not pass legislation: Delaware, Massachusetts, Minnesota, Missouri, New Jersey, New York, Ohio, Pennsylvania, South Carolina, and Washington. *See Employer Access to Social Media User Names and Passwords, 2012 Legislation*, NCSL, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx (last updated Jan.

considering five bills in the past two years, two of which are currently pending—the Password Protection Act (PPA)[14] and the Social Networking Online Protection Act (SNOPA).[15] While some similarities exist, these various state and federal pieces of legislation differ dramatically in a number of ways, including the specific prohibited acts, the definitions of important terms such as "social media" and "personal account," whether exceptions or exemptions apply, and language regarding enforcement and penalties.

This legislative development is fascinating, particularly because it moves against the otherwise prevailing belief that employee privacy is on the decline.[16] Nonetheless, a significant number of state legislatures clearly believe this protection is necessary, and rightly so. In a world where online privacy is increasingly in question, these statutes are necessary to help strike a better balance between an employer's legitimate business interests and the employee's right to keep personal information private. They are also a healthy step toward reinstating some of the privacy interests employees have lost over the years, particularly due to the development of new workplace technology that makes monitoring and access to private information easier.[17] However, these statutes certainly have their share of criticism, some of which is valid. Generally, those critical of the legislation

17, 2013). In 2013, eighteen states joined the list of those who considered similar legislation but did not pass a bill: Arizona, Connecticut, Georgia, Hawaii, Iowa, Kansas, Louisiana, Maine, Mississippi, Montana, Nebraska, New Hampshire, North Carolina, North Dakota, Rhode Island, Texas, Vermont, and Wisconsin. *See Employer Access to Social Media User Names and Passwords*, *2013 Legislation*, NCSL, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx#2013 (last updated Feb. 21, 2014). For pending bills in 2014, see *infra* note 39.

[14]H.R. 2077, S. 1426, 113th Cong. (2013).

[15]H.R. 537, 113th Cong. (2013).

[16]*See, e.g.*, Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 Akron L. Rev. 331, 337 (2010) ("The lack of adequate protections for employees' right to privacy from employer technological monitoring has been well documented by numerous scholars."); Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. Marshall L. Rev. 83, 84 (2008) ("Employees have virtually no privacy."); Robert Sprague, *From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace*, 25 J. Marshall J. Computer & Info. L. 1, 34 (2007) (noting that "[h]istorically, courts have considered employees to have minimal expectations of privacy in the workplace").

[17]*See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 Am. Bus. L.J. 285, 289–90 (2011) ("Unfortunately, the American legal system has failed to: (1) keep up with today's powerful monitoring technology and (2) provide the necessary privacy protection to employees.").

believe either that password protection is simply unnecessary or that individual statutes are inadequate.[18] Additionally, the differences from state to state are significant enough that they will likely pose real challenges to multistate employers as they attempt to navigate them.

These laws are so recent that no cases have yet challenged their application. To date, only a small number of published articles have analyzed this trend, and none have introduced any model legislation.[19] This article fills that gap. It examines the current legislation, both enacted and proposed. It argues in favor of these laws, generally, but shows that no current statute or bill adequately balances the need for employers to investigate and monitor job applicants and current employees while also recognizing their privacy interests. Therefore, this article proposes model language that should form the basis for a federal statute. In doing so, it also adds to the call from scholars about the need for comprehensive federal legislation to address employee Internet privacy.[20]

---

[18]*See infra* Part II.B.

[19]*See, e.g.*, Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 J. High Tech. L. 42 (2014); Poore, *supra* note 8; Robert Sprague, *No Surfing Allowed: A Review and Analysis of Legislation Prohibiting Employers from Demanding Access to Employees' and Job Applicants' Social Media Accounts*, 24 Alb. L.J. Sci. & Tech. (forthcoming 2014), *available at* http://ssrn.com/abstract=2390256; 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 (2013) (analyzing in brief six state statutes and making general suggestions for federal legislation); Courteney B. Lario, Note, *What Are You Looking At?: Why the Private Sector's Use of Social Media Need Not Be Legislated*, 38 Seton Hall Legis. J. 133 (2013); Sarah N. O'Donohue, Note, *"Like" It or Not, Password Protection Laws Could Protect Much More than Passwords*, 20 J.L. Bus. & Ethics 77 (2014); Michelle Scheinman, *Cyberfrontier: New Guidelines for Employers Regarding Employee Social Media*, 44 McGeorge L. Rev. 731 (2013) (examining existing law that may already prohibit asking for social media access and analyzing the California statute); Rachel M. South, *House Bill 117: Labor; Employees Requesting Username, Password or Means of Accessing an Account for Purposes of Accessing Personal Social Media; Prohibit*, 6 J. Marshall L.J. 717 (2013) (summarizing proposed Georgia H.B. 117). Buckley (*supra*) and Poore (*supra* note 8) include suggestions for language that appropriate legislation should contain, but do not provide an entire model statute.

[20]*See, e.g.*, Levinson, *supra* note 16, at 335 ("Perhaps most significantly, few, if any, academic articles have proposed an actual draft of legislation designed to protect employees from technological monitoring by their employers. Yet if recent calls for privacy protection to address emerging technologies are to succeed, blueprints for legislation must be provided."); Laura Arredondo-Santisteban, Note, *Stealing Glances: Electronic Communications Privacy and the Necessity for New Legislation in the Digital Age*, 14 N.C. J.L. & Tech. Online 205, 235 (2013), *available at* http://ncjolt.org/wp-content/uploads/2013/06/Arredondo_Final.pdf ("A uniform federal approach should encompass the password protection statutes that have currently

After this Introduction, Part I summarizes the general provisions of the currently enacted state statutes. It includes, where appropriate, discussion of the proposed state and federal bills, particularly those that add unique provisions. Part II discusses the necessity for this legislation to ensure protection of employee privacy and responds to the major criticisms of these laws. Part III sets forth a Proposed Act that should form the basis of future legislation. It then explains the considerations that went into the proposal, including how it is intended to resolve problems associated with the current state laws.

I. Current Legislation

In 2012, four states—California,[21] Illinois,[22] Maryland,[23] and Michigan[24]—enacted laws that generally prohibit an employer from requiring a job applicant or current employee to disclose a username or password for his or her social media account.[25] In 2013, eight more states—Arkansas,[26] Colorado,[27] Nevada,[28] New Jersey,[29] New Mexico,[30]

---

been adopted by several states and expand upon those protections to include other forms of access to stored communications. Federal legislation should act as a prohibition against all unauthorized access, regardless of whether a password was requested or demanded for access.").

[21]Cal. Lab. Code § 980 (West 2012).

[22]820 Ill. Comp. Stat. Ann. 55/10 (West 2012).

[23]Md. Code Ann., Lab. & Empl. § 3-712 (West 2012).

[24]Mich. Comp. Laws Ann. §§ 37.271–278 (West 2012).

[25]Many of these states, such as California and Utah, also enacted provisions to prohibit academic institutions from requiring password or login credentials from students. Although a related topic, legislation related to academic institutions is beyond the scope of this paper.

[26]Ark. Code Ann. § 11-2-124 (West 2013).

[27]Colo. Rev. Stat. Ann. § 8-2-127 (West 2013).

[28]Nev. Rev. Stat. Ann. § 613.135 (West 2013).

[29]N.J. Stat. Ann. §§ 34:6B-5–10 (West 2013).

[30]N.M. Stat. Ann. § 50-4-34 (West 2013).

Oregon,[31] Utah,[32] and Washington[33]—passed similar statutes. As of mid-2014, Louisiana,[34] Oklahoma,[35] Rhode Island,[36] Tennessee,[37] and Wisconsin[38] have enacted, and a total of twenty-seven other states[39] and Congress[40] have considered, similar legislation. Thus, in just the past three years, a majority of states (forty-four) and both the U.S. House of

---

[31]Or. Rev. Stat. Ann. § 659A.330 (West 2014).

[32]Utah Code Ann. §§ 34-48-101–301 (West 2013).

[33]Wash. Rev. Code Ann. §§ 49.44.200, 205 (West 2013).

[34]2014 La. Act 165 (to be codified at La. Rev. Stat. Ann. 51:19511955 (2014)).

[35]H.B. 2372, Reg. Sess. (Okla. 2014) (to be codified at Okla. Stat. Ann. tit. 40, §§ 173.2, 173.3 (West 2014)) (effective Nov. 1, 2014).

[36]2014 R.I. Pub. Law S2095A (to be codified at R.I. Gen. Laws Ann. § 28-56-1–6 (West 2014) (effective June 30, 2014).

[37]Wis. Stat. Ann. § 995.55 (West 2014).

[38]Tenn. Pub. Act No. 2014-826 (effective Jan. 1, 2015).

[39]The twenty-seven states that have or are considering, but have not yet passed, legislation are Arizona, Connecticut, Delaware, Florida, Georgia, Hawaii, Indiana, Iowa, Kansas, Maine, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New York, North Carolina, North Dakota, Ohio, Pennsylvania, South Carolina, Texas, Vermont, West Virginia, and Wyoming. *See Employer Access to Social Media User Names and Passwords*, *2014 Legislation*, NCSL, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014 (last updated May 14, 2014). Rather than passing password protection legislation, the Vermont legislature created a "Social Networking Privacy Protection Study Committee" whose task was to study the issue, including laws enacted or proposed elsewhere, and make recommendations by January, 2014. S. 7, Act 47, 2013–2014 Leg. Sess. (Vt. 2013) (codified at 21 Vt. Stat. Ann. tit. 21, § 495(j) (2013)). In its January 14, 2014, report, the committee reported that its "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, Social Networking Privacy Study Committee Report (Act 47 of 2013), 2013–2014 Leg. Sess. (2014), *available at* http://www.leg.state.vt.us/reports/2014ExternalReports/296108.pdf. Similar to Vermont, Maine voted to suspend its "social media privacy" bill, L.D. 1194, and form a committee to "study the issues involved in social media and personal e-mail privacy with regard to education and employment." L.B. 1194 Amendment C-A (H-640), 126th Maine Leg., 2d Reg. Sess. (Me. 2014). Wyoming's proposed legislation, introduced February 10, 2014, met a quick end when it was indefinitely postponed on February 26. S.F. 81, 62d Leg., 2014 Budget Sess. (Wyo. 2014).

[40]*See* supra notes 14 & 15 and accompanying text.

Representatives and U.S. Senate have either enacted or considered enacting employee password protection legislation.[41]

Most lawmakers in favor of the legislation claim it is necessary to protect employee privacy. Nebraska State Senator Tyson Larson, who introduced a bill in the Nebraska House of Representatives in 2013, indicated that the legislation was necessary to protect individual privacy because of the increasing popularity of social media. Noting that social media users often take advantage of the websites' privacy settings to limit access to their posts, Senator Larson stated that "[i]nformation that is kept private by an employee or applicant should remain private, and an employer should not be entitled to access this private information just because it is kept on the Internet."[42] Other legislators who introduced similar legislation expressed comparable justification for their bills.[43] However, while the underlying purpose of these laws is relatively the same from state to state, and some legislators have clearly modeled their proposed bills on earlier legislation, the statutes themselves still vary

---

[41]The six states that have not considered this issue are Alabama, Alaska, Idaho, Kentucky, South Dakota, and Virginia.

[42]*Hearing on LB 58 Before the Business and Labor Committee*, 103d Leg., 1st Sess. (Neb. 2013) (Statement of Sen. Tyson Larson, Member, Sen. Comm. on Bus. and Labor).

[43]*See* David Kravets, *6 States Bar Employers from Demanding Facebook Passwords*, WIRED (Jan. 2, 2013, 2:24 PM), http://www.wired.com/threatlevel/2013/01/password-protected-states/ ("'Our social-media accounts offer views into our personal lives and expose information that would be inappropriate to discuss during a job interview due to the inherent risk of creating biases in the minds of employers,' [California Assemblywoman Nora] Campos said. 'In order to continue to minimize the threat of bias and discrimination in the workplace and the hiring process, California must continue to evolve its privacy protections to keep pace with advancing technology.'"); Brendan Sasso, *Lawmakers Seek to Bar Bosses from Asking for Facebook Passwords*, THEHILL (May 22, 2013, 4:40 PM), http://thehill.com/blogs/hillicon-valley/technology/301319-lawmakers-look-to-bar-bosses-from-asking-for-facebook-passwords ("Without this protection, employers essentially can act as imposters and assume the identity of an employee and continually access, monitor and even manipulate an employee's personal social activities and opinions.") (quoting Rep. Ed Perlmutter (D-CO), co-sponsor of the PPA) (internal quotation marks omitted); Bob Sullivan, *EXCLUSIVE: "SNOPA" Would Ban Employers, Schools from Demanding Facebook Passwords*, NBC NEWS.COM (Apr. 27, 2012, 11:37 AM), http://www.nbcnews.com/technology/exclusive-snopa-would-ban-employers-schools-demanding-facebook-passwords-738965 ("We have to draw a line between what is publicly available information, and what is personal, private content. I think we would all object to having to turn over usernames and passwords for email accounts, or even worse, to bank accounts. User-generated social media content should be no different.") (quoting Rep. Eliot Engel (D-N.Y.), who introduced SNOPA) (internal quotation marks omitted).

significantly, which makes analysis a daunting task. Indeed, the statutes are so diverse and numerous that a detailed discussion of each would be unproductive and of little value.[44] Therefore, this section provides a general overview rather than an exhaustive analysis of each state statute, primarily to introduce the general provisions and to exemplify why model legislation would be a useful step toward uniformity. It focuses mainly on the seventeen enacted laws rather than proposed bills, although it also includes discussion of provisions found in proposed legislation that are unique or upon which the Proposed Act relies. The following brief summary of the enacted legislation and a few select bills is organized into six broad categories: (1) the parties to whom the statutes apply, (2) the applicable online accounts, (3) prohibited acts, (4) exemptions or exceptions, (5) enforcement provisions, and (6) unique provisions. The table in Appendix A details each enacted statute and selected proposed bills. The statutes and proposed bills that form the basis of the Proposed Act are also discussed in more detail later in Part IV.B.

Most of the statutes apply to employers, employees, and job applicants.[45] Although many do not define those terms, the term "employer" generally includes both public and private employers.[46] One proposed bill also included independent contractors within the definition of "employee."[47]

One of the more interesting and controversial differences between the statutes relates to the type of online account or device the employer may (or may not) access.[48] Some statutes are limited only to "social

---

[44]The total number of state and federal bills, either enacted or introduced, is at least seventy-five. This number does not include bills that were introduced but rejected in those seventeen states that have enacted a statute, nor does it include amended bills.

[45]*See, e.g.*, Colo. Rev. Stat. Ann. § 8-2-127(1)(a) (West 2013); Mich. Comp. Laws Ann. § 37.272(c) (West 2012). The exception is the New Mexico statute, which applies only to prospective employees. *See* N.M. Stat. Ann. § 50-4-34(A) (West 2013).

[46]*See, e.g.*, Ark. Code Ann. § 11-2-124(a)(2) (West 2013); Utah Code Ann. § 34-48-102(2) (West 2013).

[47]*See* L.B. 1194, 2013 Leg., 1st Reg. Sess. (Me. 2013). The proposed bill does not define the term "independent contractor."

[48]Indeed, the definitions of "social media" and "personal accounts" may be the most controversial portions of these statutes, beyond, of course, their very existence. The concept of "ownership" of social media or online accounts is an emerging issue in employment law. *See infra* text accompanying notes 122–134.

networking website"[49] while others extend more broadly to some variation of the term "online personal account."[50] Of those that do define the relevant terms (some do not), the definitions themselves are often strikingly different. For example, consider the difference between the Michigan and Utah statutes. Michigan defines a "personal internet account" as one that is "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."[51] Notably, however, this definition does not make clear why the account is personal to the user, nor does the statute refer elsewhere to a "nonpersonal account" from which one might infer the meaning of the term "personal." On the other hand, Utah illuminates the personal nature of the accounts to which its law refers by defining a "Personal Internet account" as an "online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer."[52] Statutes that cover either social media or personal online accounts can be differentiated from those that focus more upon the type of device through which such accounts might be accessed. For instance, the Colorado statute prohibits employers from asking for access to a personal account or service "through the employee's or applicant's electronic communications device."[53] Given this variety, clearly the applicable mediums or devices contemplated by these laws are far from uniform.

---

[49]*See, e.g.*, 820 Ill. Comp. Stat. Ann. 55/10(b)(1) (West 2012); N.M. Stat. Ann. § 50-4-34(E).

[50]*See, e.g.*, Colo. Rev. Stat. Ann. § 8-2-127(2)(a); Mich. Comp. Laws Ann. § 37.272(d).

[51]Mich. Comp. Laws Ann. § 37.272(d).

[52]Utah Code Ann. § 34-48-102(4)(a) (West 2013); *see also* Wis. Stat. Ann. § 995.55(1)(d) (West 2014). *Compare also* 820 Ill. Comp. Stat. 55/10(b)(4)(A)–(C) (defining "social networking website" as 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"), *with* Cal. Lab. Code § 980(a) (West 2012) (defining "social media" 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, email, online services or accounts, or Internet Web site profiles or locations").

[53]Colo. Rev. Stat. Ann. § 8-2-127(2)(a). *See also* Md. Code Ann., Lab. & Empl. § 3-712(a)(3)(i) (West 2012) (defining "Electronic communications device" as including "computers, telephones, personal digital assistants, and other similar devices").

The statutes are most consistent regarding the acts the laws prohibit. Each of the statutes and bills essentially prohibits employers from requiring a job applicant or employee to disclose or provide a username, password, or other login credentials that would allow access to the applicant's or employee's social media or personal online account.[54] A few go further and prohibit indirect access such as observation of the account in the presence of the employee[55] (sometimes referred to as "shoulder surfing"[56]), changing privacy settings to allow public observation of the profile's contents,[57] or adding the employer or an agent to the employee's or applicant's contact list.[58] A majority of the enacted statutes also prohibit retaliation against employees or job applicants who refuse to provide the employer with requested login credentials.[59]

Summarizing the many different exceptions found within the statutes and proposed bills is a difficult task because they vary considerably, ranging from those statutes that have only a few exceptions[60] to a much broader framework of exemptions.[61] Exceptions generally include provisions that allow employers to investigate workplace misconduct[62] and possible misappropriation of proprietary, confidential, or financial

---

[54]*See, e.g.*, Cal. Lab. Code § 980(b)(1); Nev. Rev. Stat. Ann. § 613.135(1)(a) (West 2013); Wash. Rev. Code Ann. § 49.44.200(1)(a) (West 2013).

[55]*See, e.g.*, Or. Rev. Stat. § 659A.330(1)(c) (West 2014); Wash. Rev. Code Ann. § 49.44.200(1)(b); Wis. Stat. Ann. § 995.55(2)(a)(1).

[56]The term "shoulder surfing" generally applies to a person who observes a computer user to obtain information, often without the user's knowledge or consent. *See Shoulder Surfing*, techopedia, http://www.techopedia.com/definition/4103/shoulder-surfing (last visited May 26, 2014) ("Shoulder surfing refers to the act of obtaining personal or private information through direct observation."); *shoulder surfing*, Oxford Dictionaries, http://oxforddictionaries.com/us/definition/american_english/shoulder-surfing (last visited May 26, 2014) ("The practice of spying on the user of an ATM, computer, or other electronic device in order to obtain their personal access information.").

[57]*See, e.g.*, Ark. Code Ann. § 11-2-124(b)(1)(C) (West 2013).

[58]*See, e.g.*, Or. Rev. Stat. § 659A.330(1)(b).

[59]*See, e.g.*, Cal. Lab. Code § 980(e); Colo. Rev. Stat. Ann. § 8-2-127(3)(a) & (b) (West 2013).

[60]*See, e.g.*, N.M. Stat. Ann. §§ 50-4-34(B)(1)–(2), (C) & (D) (West 2013).

[61]*See, e.g.*, Utah Code Ann. § 34-48-201 (West 2013).

[62]*See, e.g.*, Ark. Code Ann. § 11-2-124(e)(2)(A).

information.[63] Many statutes also allow employers to search for information about employees or applicants available in the public domain[64] and to ask for login information necessary to access the employer's own networks and equipment.[65] The Wisconsin statute allows an employer to request or require an employee to disclose the employee's personal e-mail address.[66]

The laws continue to differ significantly regarding enforcement provisions and penalties. Some statutes simply do not address enforcement or possible remedies at all.[67] Others provide for only a civil remedy,[68] while Michigan alone allows for both a civil remedy and criminal enforcement.[69] The available damages range from no dollar amount indicated,[70] to $500 in Utah and Washington,[71] $1,000 in Michigan and New Jersey,[72] all the way up to $10,000 in SNOPA and one proposed bill.[73] Legislation in Colorado and Wisconsin, SNOPA, and a proposed bill in Connecticut place enforcement responsibilities on administrative agencies,[74] while,

---

[63]*See, e.g.*, Mich. Comp. Laws Ann. § 37.275(1)(b)–(c) (West 2012).

[64]*See, e.g.*, Ark. Code Ann. § 11-2-124(d).

[65]*See, e.g.*, Nev. Rev. Stat. Ann. § 613.135(2) (West 2013).

[66]Wis. Stat. Ann. § 995.55(2)(b)(7) (West 2014).

[67]Statutes in the following states do not contain a penalty provision: Arkansas, California, Illinois, Nevada, New Mexico, and Oregon.

[68]*See, e.g.*, Utah Code Ann. § 34-48-301 (West 2013); Wash. Rev. Code Ann. § 49.44.205 (West 2013).

[69]*See* Mich. Comp. Laws § 37.278 (West 2012).

[70]*See* Md. Code Ann., Lab. & Empl. § 3-712(f) (West 2012); 2014 R.I. Pub. Law S2095A (to be codified at R.I. Gen. Laws Ann. § 28-56-6 (West 2014) (effective June 30, 2014). Several proposed bills provide for a civil penalty but do not specify a dollar amount. *See, e.g.*, North Carolina (H.B. 846, 2013); New Hampshire (H.B. 1407, 2014 Leg., Reg. Sess. (N.H. 2014)); Nebraska (L.B. 58, 103d Leg., 1st Sess. (Neb. 2013) and H.B. 1455, 103d Leg., 1st Sess. (Neb. 2013)).

[71]Utah Code Ann. § 34-48-301(2); Wash. Rev. Code Ann. § 49.44.205(1).

[72]Mich. Comp. Laws Ann. § 37.278(2); N.J. Stat. Ann. § 34:6B-9 (West 2013). The New Jersey law awards $2,500 for each subsequent violation. *Id.* Colorado also increases the penalty, to $5,000, for each subsequent violation. Colo. Rev. Stat. Ann. § 8-2-127(5) (West 2013).

[73]*See* H.R. 537(b)(1)(A), 113th Cong. (1st Sess. 2013); S.B. 159, 2013 Gen. Assemb., Jan. Sess. (Conn. 2013).

[74]*See* Colo. Rev. Stat. Ann. § 8-2-127(5) (providing that claims shall be filed with the state department of labor and employment); Wis. Stat. Ann. § 995.55(6)(b) (West 2014) (allowing

conversely, at least one other state bill intentionally excludes enforcement obligations from the relevant agency.[75]

A handful of unique provisions found in particular statutes or bills are worth mentioning. Placement of these laws within the state code is widely varied; some laws are found in an entirely new act,[76] while others amend or add to existing labor statutes.[77] New Jersey is the first enacted law that expressly prohibits the employer from asking an employee or applicant to waive protection provided by the law; it also provides that any agreements to waive the provisions are unenforceable.[78] The recently enacted statute in Louisiana does not prohibit an employee or applicant from "self-disclosing" username or password information that allows the employer to access a personal online account.[79] Some state laws specifically provide that the laws do not create a duty to search or monitor employee Internet use through personal accounts, nor will employers be liable for failure to do so.[80] On the other hand, other statutes state that their

---

an employee or applicant to file a complaint with the department of workforce development); H.R. 537(b)(1)(B) (placing enforcement responsibility on the U.S. Secretary of Labor); S.B. 159 (requiring the Connecticut Attorney General to file a claim for violation of the law in Superior Court).

[75]*See* CAL. LAB. CODE § 980, Sec. 2 of Stats. 2012, c. 618 (A.B. 1844) (West 2012) ("[T]he Labor Commissioner, who is Chief of the Division of Labor standards enforcement, is not required to investigate or determine any violation of this act.").

[76]*See, e.g.*, UTAH CODE ANN. § 34-48-101 (creating the "Internet Employment Privacy Act").

[77]*See, e.g.*, CAL. LAB. CODE § 980; N.M. STAT. ANN. § 50-4-34 (West 2013) (amending existing Article 4 "Labor Conditions; Payment of Wages").

[78]N.J. STAT. ANN. § 34:6B-7 (West 2013) ("No employer shall require an individual to waive or limit any protection granted under this act as a condition of applying for or receiving an offer of employment. An agreement to waive any right or protection under this Act is against the public policy of this State and is void and unenforceable."). *See also* H.B. 1455, 103d Leg., 1st Sess. (Neb. 2013); L.B. 58, 103d Leg., 1st Sess. (Neb. 2013).

[79]*See* 2014 La. Act 165 (to be codified at LA. REV. STAT. ANN. 51:1953(G) (2014)).

[80]*See, e.g.*, MICH. COMP. LAWS ANN. § 37.277(1) (West 2012) ("This act does not create a duty for an employer . . . to search or monitor the activity of a personal internet account."); *id.* § 37.277(2) ("An employer . . . is not liable under this act for failure to request or require that an employee. . . [or] an applicant for employment. . . grant access to, allow observation of, or disclose information that allows access to or observation of the employee's. . . [or] applicant for employment's. . . personal internet account."); UTAH CODE ANN. § 34-48-203(1)–(2); *see also* OR. REV. STAT. § 659A.330(3) (West 2014) (providing that "[a]n employer may not be held liable for the failure to request or require an employee or applicant to disclose the information specified" in the act).

provisions are not intended to hinder any other legal duty to conduct Internet searches on employees or job applicants.[81]

This concludes a broad summary of the legislation relating to an employer's access to employees' and applicant's social media and online accounts, both enacted and proposed. The Proposed Act incorporates many of the provisions discussed in this section, as is explained more fully in Part III below. However, before considering the Proposed Act, this article first considers why this legislation is important. It also addresses and responds to critics of the laws.

II. The Need for Balanced, Comprehensive Legislation to Protect Internet Privacy Rights

Clearly, employers have a legitimate interest in gaining information about employees and job applicants. Employers monitor employees' and job applicants' online behavior to learn about their character, personality traits, and interests that may have bearing on their ability to do the job.[82] Employers also have compelling business reasons to pay attention to current employees' productivity, work performance, and possible security violations.[83] Moreover, "[f]ailure to uncover an obvious flaw in an employee's background or character could lead to negligent hiring and negligent retention lawsuits or malpractice claims having serious business

---

[81]*See, e.g.*, Mich. Comp. Laws Ann. § 37.275(2) (providing that the "act does not prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under federal law or by a self-regulatory organization").

[82]*See* Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 Am. Bus. L.J. 63, 69–70 (2012).

[83]*See id*. at 70; *see also* Michael Z. Green, *Against Employer Dumpster-Diving for Email*, 64 S.C. L. Rev. 323, 335 (2012) ("[E]mployers have legitimate reasons to want information about their employees, including the need to address concerns about harassment, theft, protection of trade secrets, and efficient performance of duties. Sometimes employers may need to investigate and review an employee's ESI [electronically stored information] either as part of the employer's duties to act responsibly under law or as an attempt to protect itself in litigation.") (footnote omitted); Robert Sprague, *Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship*, 50 U. Louisville L. Rev. 1, 7–9 (2011) (discussing various potential legal liabilities employers may face for not properly vetting job candidates).

repercussions."[84] However, despite these reasonable concerns, intrusions into employee privacy can also damage employee morale and the employment relationship,[85] a reality employers may often ignore.[86] Further, although employees generally accept that they will be monitored at work, research indicates that few of those applicants believe their online information will have an impact on a decision to hire them.[87] Young people in particular "still cling to certain expectations of privacy in the workplace."[88] This is hardly surprising, given how the right to privacy has ebbed in recent years.[89]

---

[84]Abril et al., *supra* note 82, at 70 (footnotes omitted).

[85]*Id*. at 69 ("A considerable body of business research indicates that employer invasiveness may lead to higher levels of employee stress, lower levels of productivity, and worse employee health and morale."); Ciocchetti, *supra* note 17, at 286–87 ("[E]mployee monitoring pierces the veil of an individual's privacy and can decrease morale.").

[86]*See* John Soma et al., *Bit-Wise but Privacy Foolish: Smarter E-Messaging Technologies Call for a Return to Core Privacy Principles*, 20 Alb. L.J. Sci. & Tech. 487, 493 (2010) (noting "there is increasing evidence that employers often ignore the adverse consequences to employee morale and occupational health" arising from surveillance technologies) (internal quotation marks omitted).

[87]Kabrina K. Chang, *All Up in Your Facebook: Using Social Media to Screen Job Applicants*, 47 New Eng. L. Rev. On Remand 1, 2 (2012), *available at* http://newenglrev.com/on-remand-2/volume-47-on-remand/chang-all-up-in-your-facebook/ (citing a 2009 study in which only nine percent of those surveyed believed employers would make hiring decisions based upon their online activity); *see also* Jean M. Roche, Note, *Why Can't We Be Friends?: Why California Needs a Lifestyle Discrimination Statute to Protect Employees from Employment Actions Based on Their Off-Duty Behavior*, 7 Hastings Bus. L.J. 187, 190–91 (2011).

[88]Abril et al., *supra* note 82, at 73.

> Millennials seem to take for granted that their work and personal lives do *not* intersect and that their actions in one should *not* affect the other, as marked by their overwhelming belief that an employee's conduct outside the office should not be used as a basis for making promotion determinations. Their objection to this increasingly common practice reflects an expectation that they would not be discriminated against on the basis of their online identities.

Id. at 108 (emphasis in original) (footnote omitted); *see also* Allyson W. Haynes, *Virtual Blinds: Finding Online Privacy in Offline Precedents*, 14 Vand. J. Ent. & Tech. L. 603, 642 (2012).

[89]*See, e.g.*, *supra* text accompanying note 16; *see also* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 Berkeley Tech. L.J. 979, 1018 (2011) ("[E]mployees should anticipate very minimal expectations of privacy in workplaces within the United States."); Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 Chi.-Kent L. Rev. 901, 903 (2012) ("[M]any commentators have argued that employee privacy is insufficiently protected in the electronic workplace.").

A wide variety of interested parties, including scholars, practitioners, courts, and legislatures, have deliberated over where the appropriate line between these two competing interests should be drawn. Whether and to what degree employees and job applicants have, or should have, any expectation of privacy regarding their online accounts is a "vexing" contemporary question,[90] indicating that the rights of both employers and employees are far from clear.[91] Although many scholars acknowledge that the privacy pendulum has swung in favor of employers, "[t]he extent to which the law should intervene in the employment relationship to protect employee privacy is highly contested."[92] Passage of legislation that prohibits unwarranted intrusion into employees' and job applicants' personal online accounts helps answer this vexing question regarding employee Internet privacy. It is an important and necessary step toward providing both employers and employees with clearer boundaries regarding what is, and is not, acceptable at work. From a broader perspective, this legislation will also be a useful tool upon which courts can rely as they attempt to clarify privacy interests in social media and other online accounts.

A. Password Protection Legislation Clarifies the Law Regarding Employee Internet Privacy

When considering whether employees and applicants have a reasonable expectation of privacy in their personal online accounts, one must first acknowledge that most social media websites allow users to communicate in a number of ways. A person's "digital footprint" usually contains far more than simply posts made on a page that are visible to every one of that person's contacts and to the public. A social media profile in particular is often a highly personal record of that user's life, related to activities the

---

[90]Zoe Argento, *Whose Social Network Account? A Trade Secret Approach to Allocating Rights*, 19 Mich. Telecomm. & Tech. L. Rev. 201, 235 (2013).

[91]*See* Francois Quintin Cilliers, *The Role and Effects of Social Media in the Workplace*, 40 N. Ky. L. Rev. 567, 568–69 (2013) ("The lack of statutes and regulations regarding the usage of social media in the hiring process creates uncertainty for employers and employees."); Kim, *supra* note 89, at 902 ("[T]he norms surrounding whether or when employees can expect privacy in their communications are highly uncertain."); Nancy B. Schess, *Then and Now: How Technology Has Changed the Workplace*, 30 Hofstra Lab. & Emp. L.J. 435, 452 (2013) ("Uncertainty in the law is particularly evident in the context of employee use of social media.").

[92]Kim, *supra* note 89, at 903 (emphasis omitted).

user engages in outside of work, much of which can be kept private from the viewing public. Users who are connected to each other in social media platforms such as Facebook and LinkedIn may communicate via private messages, which are akin to e-mail.[93] They may also share information by posting on their own "walls" or profile pages, but those posts are not necessarily available to the public or even to the user's entire contact list.[94] Facebook, for instance, provides a multitude of privacy options that allow users to select a specific audience for posted content. These selections include visibility to only the user, to one or a few of the user's friends, to only the user's entire friend list, or to the public.[95] Employers who have unfettered access to employees' or applicants' social media profiles that contain any combination of the above are likely to intrude into personal, off-work areas of the employees' or applicants' lives where, arguably, they have a reasonable expectation of privacy.[96] However, given the variety of methods by which users can communicate with each other on social media websites, the question then becomes where specifically that reasonable expectation of privacy begins and ends. May a user expect privacy in private messages? In public posts? In posts made viewable to only a few users? Although we can look to analogous areas of law for guidance, answers to these questions remain murky at best. Piecemeal application of existing law to social media creates a quagmire employers may be unlikely to negotiate well.

---

[93]*See infra* text accompanying notes 97–104.

[94]*Buckley*, *supra* note 19, at 877 ("The configuration of social media websites typically permits users to choose between various methods of communication to interact. These choices enable users to dictate the parameters of their audiences.").

[95]*See Facebook Basic Privacy Settings & Tools*, Facebook, http://www.facebook.com/help/325807937506242 (last visited May 26, 2014).

[96]Many scholars and commentators have argued that employees have, or should have, a reasonable expectation of privacy regarding their off-work activities. *See, e.g.*, Marisa Anne Pagnatarro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. Pa. J. Lab. & Emp. L. 625, 629–77 (2004); Jason Bosch, Note, *None of Your Business (Interest): The Argument for Protecting All Employee Behavior with No Business Impact*, 76 S. Cal. L. Rev. 639, 660 (2003); Shelbie J. Byers, Note, *Untangling the World Wide Weblog: A Proposal for Blogging, Employment-At-Will, and Lifestyle Discrimination Statutes*, 42 Val. U. L. Rev. 245, 255 (2007); Joseph Lipps, Note, *State Lifestyle Statutes and the Blogosphere: Autonomy for Private Employees in the Internet Age*, 72 Ohio St. L.J. 645, 685 (2011); Ann L. Rives, Note, *You're Not the Boss of Me: A Call for Federal Lifestyle Discrimination Legislation*, 74 Geo. Wash. L. Rev. 553, 568 (2006); Roche, *supra* note 87, at 190–91.

Private messages sent between social media users are the functional equivalent of private e-mail from personal accounts,[97] in which several recent cases have held that users generally have a reasonable expectation of privacy. In *Stengart v. Loving Care Agency, Inc.*,[98] the New Jersey Supreme Court found that an employee had a reasonable expectation of privacy in e-mails she exchanged with her attorney and accessed through a work computer because she took precautions to ensure her privacy, even though the company notified employees of its policy that their personal e-mail messages accessed through company equipment would not be private. The court noted, in particular, that Stengart had used a personal, password-protected e-mail account instead of her company e-mail address.[99]

The District Court for the Southern District of New York reached a similar holding in *Pure Power Boot Camp v. Warrior Fitness Boot Camp*[100] involving an employer who opened and printed several e-mails from a former employee's personal account, using password information the employee had stored on his work computer. Concluding that the employer violated the Stored Communications Act[101] (SCA) by accessing the employee's online account without authorization, the court found that the employee "had a subjective belief that his personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords, would be private."[102]

---

[97]*See* Allen D. Hankins, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 Suffolk. J. Trial & App. Advoc. 295, 315 (2012) ("Private messaging on Facebook functions very similarly to web-based e-mail."); Ryan A. Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 Harv. J.L. & Tech. 563, 571–72 (2011).

[98]990 A.2d 650 (N.J. 2010).

[99]*Id.* at 663 (concluding plaintiff had a subjective expectation of privacy in her e-mail messages).

[100]587 F. Supp. 2d 548 (S.D.N.Y. 2008).

[101]Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–11 (2012)). The SCA comprises Title II of the Electronic Communications Privacy Act (ECPA), which itself was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968).

[102]*Pure Power Boot Camp*, 587 F. Supp. 2d at 561. The court further concluded the employee's privacy expectation was reasonable because nothing in the employer's e-mail policy indicated it would extend beyond the employer's systems or the employment relationship; nor had the policy been clearly communicated to the employees. *Id.*

Another case considered whether the SCA applies to private messages sent via social networking. In *Crispin v. Christian Audigier, Inc.*, the District Court for the Central District of California held there "is no basis for distinguishing between . . . Facebook's and MySpace's private messaging, on the one hand, and traditional web-based email on the other."[103] As such, the *Crispin* court found that the SCA did apply to the private messages at issue in the case, thus limiting the defendant's right to access those communications via subpoena.[104]

Although these cases support employee privacy in private social media messages, they may be limited. For example, at least one practitioner points out that *Stengart*'s precedent is "narrow" because it relied in part on the fact that the communication in question was privileged since it involved correspondence with an attorney, which will not be a factor in most situations in which employees conduct personal business on work computers. "As a result, *Stengart v. Loving Care* is a fig leaf precedent: it provides slight but valuable protection of something superlatively private and leaves everything else exposed."[105] Additionally, at least one other court has reached a conclusion opposite to the *Stengart* and *Pure Power Boot Camp* decisions. In an unpublished opinion, the Texas Court of Appeals rejected an employee's tort claim of invasion of privacy based on intrusion upon seclusion.[106] The court held that the employee had no reasonable expectation of privacy in items stored on the employer's computer, even though password protected, because the information was transmitted over the employer's network and accessible by the employer.[107] Also, even

---

[103]717 F. Supp. 2d 965, 981–82 (C.D. Cal 2010). The court also "differentiated between read and unread private messages, holding that they are protected in different ways under the SCA." Ward, *supra* note 97, at 571. This technical difference between read and unread e-mail messages contributes to the problems related to applying the SCA to employer requests for password information. *See infra* text accompanying notes 173–177.

[104]*Crispin*, 717 F. Supp. 2d at 991.

[105]Brent A. Crossrow, *The Fig Leaf Precedent Set by* Stengart v. Loving Care Agency, Inc., 10 Bloomberg Law Reports—Technology Law, no. 2, 2010, *available at* http://www.laborlawyers.com/files/25559_the%20fig%20leaf%20precedent%20set%20by%20ste.pdf.

[106]McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. Ct. App. May 28, 1999).

[107]*Id.* at *4. *See also* Holmes v. Petrovich Dev. Co., 19 Cal. Rptr. 3d 878 (Cal. Ct. App. 2011) (holding employee had no expectation of privacy in e-mails sent to her attorney through the employer's computer system).

assuming the employee did have a reasonable expectation of privacy in the content in question, the court found that the employer's interception of it was not a highly offensive invasion because of the employer's legitimate interest in preventing illegal and unprofessional activity on its equipment.[108]

Accordingly, an employee or applicant *might* have a persuasive argument that an employer who asks for a password to an online social media account may not access private messages within the employee's or applicant's profile, at least absent an explicit policy that notifies employees that the employer may do this.[109] However, users usually communicate on the main page of their online profiles as well. Some of those posts may be set for public viewing. Others might be limited to only the user's contacts, perhaps even just a few of them. Would the expectation of privacy in personal e-mail messages as contemplated in *Stengart, Pure Power Boot Camp*, and *Crispin* extend to these wall posts as well? The answer to this question is important because an employer who requires access to a personal social media profile will see these posts directly upon logging in.

Some commentators have advanced the argument that those who make an effort to protect the privacy of their online accounts should be able to expect some reasonable expectation of privacy in that content. "Reliance on protections such as individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable."[110] "This reasoning would provide a greater expectation of privacy in password-protected or limited-access social networking profiles."[111]

Until recently, this approach to privacy was just barely reflected in case law. "[C]ourts have given little privacy protection to postings on an internet forum or chat room, or to other information posted to a

---

[108]*McLaren*, 1999 WL 339015 at *5; *see also* Green, *supra* note 83, at 344–45.

[109]*See* Determann & Sprague, *supra* note 89, at 1018 ("[C]ourts, particularly the U.S. Supreme Court, have shied away from acknowledging a core privacy right that employers cannot destroy by way of notice.").

[110]Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995).

[111]Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 Rich. J.L. & Tech. 1, 35 (2011); *see also* Haynes, *supra* note 88, at 641 ("[P]rivacy settings are on the rise, and courts should give them effect.").

website."[112] Considering whether an employer improperly invaded an employee's privacy by accessing her private Facebook posts without authorization, the New Jersey District Court, in *Ehling v. Monmouth-Ocean Hospital Service Corp.* (*Ehling I*), noted some consistency in case law at two ends of the privacy spectrum: no reasonable expectation of privacy for material posted to an unprotected website, in contrast to a reasonable expectation of privacy for individual, password-protected communications.[113] The *Ehling I* court noted, however, that courts have yet to develop a coherent approach between these two extremes.[114]

Although not quite the "coherent approach" contemplated in *Ehling I*, emerging case law supports an argument that social media users who attempt to safeguard the privacy of their profiles should enjoy some corresponding right to privacy. In what will undoubtedly be an important holding in social media law, in the next iteration of the *Ehling* case, *Ehling II*, the court put itself squarely at "one end of the spectrum," finding that the plaintiff's "non-public Facebook wall posts" were private and therefore covered by the SCA because she "chose privacy settings that limited access to her Facebook wall to only her Facebook friends."[115] Another oft-cited case involving employer access to password-protected electronic communications, *Pietrylo v. Hillstone Restaurant Group*,[116] also suggests that, at least in certain circumstances, courts will uphold a reasonable expectation of privacy in password-protected electronic content. In *Pietrylo*, a group of restaurant employees created and participated in a private MySpace chat group related to the restaurant and its managers. When one manager

---

[112]Haynes, *supra* note 88, at 638 (footnote omitted).

[113]872 F. Supp. 2d 369, 373 (D.N.J. 2012).

[114]*Id.*

[115]Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659, 669 (D.N.J. 2013). In *Ehling II*, the court dismissed the plaintiff's common law privacy claim because the evidence showed that the defendants were the passive recipients of information that they did not seek out or ask for. *Id.* at 674 ("Plaintiff voluntarily gave information to her Facebook friend, and her Facebook friend voluntarily gave that information to someone else."). The District Court for the Central District of California suggests that a Facebook user who limits access to wall posts might also expect some privacy in that content, although it did not rule definitively on the issue because the evidentiary record did not reveal the extent to which the plaintiff had relied on Facebook privacy settings. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

[116]No. 06–5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

learned of the MySpace group, he asked an employee with access for her login information so management could view it directly. The court upheld the jury's verdict that this behavior violated the SCA because the employee was coerced into providing the information, given her employment relationship.[117]

Despite some courts finding privacy protection in restricted-access communications, password protection legislation is still necessary. Social media websites allow users to communicate via private messages, which may afford those users some privacy in the content. In between those and posts set for public viewing is a wide variety of semiprivate content, about which the law is vague. An employer who obtains the applicant's or employee's login credentials will see any or all of this content, some of which the law *may* prohibit. But it may not.[118] Although persuasive and favorable, those cases that apply to private online communications will not be applicable to employees in all states anytime soon. Some of those cases may also be distinguishable based upon their unique facts. Federal password legislation would send a clear and positive message regarding employee privacy in private social media content and would be uniformly applicable to employees across the country.

The privacy interests at issue when employers ask for access into personal online accounts do not end with employees and job applicants either. Employers who gain entrance to an applicant's or employee's privacy-protected social media profile also have an opportunity to see private thoughts and content posted by others with whom the applicant or employee interacts.[119] These concerns, not to mention general online

---

[117]*Id*. at *3. *See also infra* text accompanying notes 160–179 (comparing SCA with social media access legislation).

[118]*See* Ward, *supra* note 97, at 576 ("Assuming other courts follow the approach laid out in *Crispin*, there are still many open questions about the SCA's applicability to social network content that is not inherently private. Most obviously, the *Crispin* court fails to give any real guidance on the precise requirement for SCA protection of Wall posts and other non-private message content. Must content be limited to a certain number of friends? Does content still fall under the SCA if your friends' friends can view it?").

[119]Argento, *supra* note 90, at 237 ("Private communications from members of the account holder's network to the account holder may also deserve protection. . . . For example, if a 'friend' on Facebook sends a private message to me through Facebook, it seems that the 'friend's' reasonable expectation of privacy in that message should be protected, perhaps not from me, but from unauthorized intrusions by others."); *see also* Garber, *supra* note 4 ("Snooping in someone's Facebook profile . . . implicates one's family and friends.").

etiquette,[120] suggest that both job applicants and employees and the people with whom they interact on their profile have privacy interests that should be protected. Also, much of the proposed legislation extends to other online accounts, including personal e-mail, banking, and other financial online accounts. It could even apply to online accounts related to medical records. Any of these accounts contain highly personal information, which makes the necessity for this legislation even more pronounced. The private material an employee or applicant maintains online should be no less off limits than any other nondigital content such as personal letters, diaries, bank statements, and medical records. Contrary to what opponents of the legislation contend,[121] employers have no business justification for viewing the entire contents of these types of accounts, social media or otherwise. To be blunt, much of this information accessible through these accounts is simply none of the employer's business. Without specific legislation to prohibit access to these potentially sensitive accounts, at least some employers may be tempted to gain access by requiring it.

In addition to clarifying the boundaries of privacy in employees' and job applicants' personal online accounts, the Proposed Act will provide needed guidance to employers and courts regarding the related, emerging issue of "ownership" of online accounts that employees use both professionally and personally. Two recent cases, *PhoneDog v. Kravitz*[122] and *Eagle v. Morgan*,[123] are illustrative of the issues that arise when employees use social media accounts for both personal and work-related reasons. Each case involved a dispute over rights to a social media account, and the important contacts associated with it, when an employee left the firm.

PhoneDog involved the ownership of a former employee's Twitter account. When Noah Kravitz left his employment at PhoneDog, he changed the name of his work-related Twitter account from "@PhoneDog_Noah" to "@noahkravitz" and continued to tweet to all of

---

[120]*Senators Call for Federal Probe over Employers Asking for Facebook Passwords*, Fox News (Mar. 25, 2012), http://www.foxnews.com/politics/2012/03/25/senators-call-for-federal-probe-over-employers-asking-for-facebook-passwords/ ("Not sharing passwords is a basic tenet of online conduct. Aside from the privacy concerns, Facebook considers the practice a security risk.").

[121]*See infra* text accompanying notes 136–150.

[122]No. C 11–03474 MEJ, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).

[123]No. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013).

the 17,000 followers he had attracted while employed at PhoneDog.[124] In PhoneDog's subsequent lawsuit against him for misappropriation of trade secrets, conversion, and intentional and negligent interference with prospective economic advantage, Kravitz defended the complaint by claiming that he established the account and password himself, and that he was entitled to it according to Twitter's terms of service. He also claimed that he had no employment agreement with PhoneDog that expressly provided that the account belonged to PhoneDog. The trial court refused to dismiss the case for failure to state a claim for misappropriation of trade secrets and conversion, finding that PhoneDog had made a significant claim that it owned or at least had the right to possess the account.[125] The case ultimately settled out of court.[126]

In *Eagle v. Morgan*, the plaintiff, a high-level executive at Edcomm, created and maintained a LinkedIn account that she used for both professional and personal purposes. When the company was sold, Edcomm terminated and replaced the plaintiff. It also accessed her LinkedIn account, changed the password, and replaced her name and photograph with that of her replacement.[127] Although she regained control of her account approximately one month later, the plaintiff sued Edcomm, alleging, among other claims, invasion of privacy, identity misappropriation, conversion, and interference with contract. Although the court held in her favor on several claims, it ultimately found that she had failed to prove damages.[128] The court did not directly address the question of how to determine access rights to online accounts such as the LinkedIn account at issue in the case, which was used for both personal and professional

---

[124]*PhoneDog*, 2011 WL 5415612, at *1.

[125]*Id.* at *7–9. The court granted Kravitz's motion to dismiss PhoneDog's claims for intentional and negligent interference with prospective economic advantage. *Id.* at *9.

[126]Daniel Terdiman, *Curious Case of Lawsuit over Value of Twitter Followers Is Settled*, CNET (Dec. 3, 2012), http://news.cnet.com/8301-1023_3-57556918-93/curious-case-of-lawsuit-over-value-of-twitter-followers-is-settled/. Although the details of the settlement are confidential, both parties confirmed that Kravitz retained sole ownership of the Twitter account. *Id.*

[127]*Eagle*, 2013 WL 943350, at *3.

[128]*Id.* at *17; *see also* Jessica Mendelson, *Court Issues Decision in* Eagle v. Morgan: *Employee Owns LinkedIn Account but Fails to Recover Any Damages Against Former Employer*, Trade Secrets (Apr. 3, 2013), http://www.tradesecretslaw.com/2013/04/articles/trade-secrets/court-issues-decision-in-eagle-v-morgan-employee-owns-linkedin-account-but-fails-to-recover-any-damages-against-former-employer/.

purposes, other than noting its disagreement with Edcomm's claim that it "owned" the LinkedIn account in question because "the LinkedIn User Agreement clearly indicated that the individual user owned the account."[129]

Although these cases do not provide a definitive holding that clarifies when an online account is personal rather than work related, they do indicate that courts are grappling with the issue and appear to be willing to consider a claim that employers have no right to access personal accounts, even those that are sometimes used for work-related purposes.[130] A few of the state statutes acknowledge the difference between personal and nonpersonal accounts (although the language used in some of those statutes is problematic),[131] but a majority of the statutes do not address this issue.[132] Because the issue of ownership helps determine the right of access to online accounts generally,[133] legislative attention to the concept of

---

[129]Eagle, 2013 WL 943350, at *11. *See also*, Maremont v. Susan Fredman Design Grp., Ltd., 2014 WL 812401, at *7 (N.D. Ill. Mar. 3, 2014) (holding there was an issue of fact regarding whether an employer accessed an employee's Facebook and Twitter accounts, used personally and for occasional business purposes, without authorization in violation of the SCA).

[130]Although employers could avoid disputes such as those in *PhoneDog* and *Eagle* by implementing and enforcing clear social media policies, inevitably some will not. *See* Argento, *supra* note 90, at 227 ("[T]he recent spate of cases involving disputes over rights to social network accounts is likely a harbinger of many disputes to come. . . . However, without express agreements in place, disputes over rights to an account are inevitable.").

[131]*See infra* text accompanying notes 217–223.

[132]*See supra* text accompanying notes 48–52.

[133]*See* Julie E. Judish et al., Drawing the Line Online: Employers' Rights to Employees' Social Media Accounts 2 (2012), www.pillsburylaw.com/siteFiles/Publications/AlertOctober2012Litigation_DrawingtheLineOnline_EmployersRightstoEmployeesSocialMediaAccounts.pdf ("A common theme connects the Eagle case with the recent password access legislation: the importance of defining the lines of ownership and demarcating the boundary between the professional and the personal. If Edcomm, for example, had established a LinkedIn account for its CEO's use and had asserted its property interest in the account at the outset of the employment relationship, Edcomm's CEO would have had no reasonable expectation of ownership in it. Under that scenario, Edcomm likely would not be facing trial on a misappropriation claim. Similarly, the social media password legislation definitively declares that employers and prospective employers have no right to access the social media accounts that applicants and employees have established for their personal use.").

personal versus nonpersonal accounts will help courts decide these cases in the future. It may even help courts resolve issues regarding ownership of work-related electronic devices.[134]

B. Current Law Is Insufficient to Protect Employee Internet Privacy: A Response to Critics

Critics of the social media access laws, many of whom are employment law attorneys, question the necessity for the legislation.[135] One claim is that because the practice of asking for password or login information is "deplorable," few employers are likely to engage in it.[136] Others argue that the current statutes simply go too far by either limiting employers in the exercise of their legitimate rights or granting employees more privacy than the law otherwise recognizes.[137] Finally, many claim that the legislation is unnecessary because the practice violates the websites' terms of service[138]

---

[134]*See, e.g.*, Soma et al., *supra* note 86, at 503 ("The trend towards using mobile devices, especially in professional ranks, is further complicated by device ownership issues. If the employer owns the device, then it can reasonably be assumed to be a part of the employer's computer systems. But what if an employee uses her own device to access her employer's systems? Does her expectation of privacy change if she is reimbursed by her employer for the e-messaging services that she uses to meet her work obligations? What if employer policies address personal device usage? What if they do not? These technology convergence and device ownership issues create a series of competing interests and call for a more integrated view of e-messaging by all cultural stakeholders including the law. Moreover, these issues only grow thornier as Americans' online communications increase, and the lines between home and the workplace continue to blur.") (footnote omitted).

[135]*See, e.g.*, Gordon, *supra* note 9 ("Remarkably, the Illinois bill (like the Maryland law) contains *no* legislative findings supporting the need for the law.") (emphasis in original); Hyman, *supra* note 9 ("I've said it before and I'll say it again, this is not a problem that needs fixing."); Torphy-Donzella, *supra* note 9 ("What is remarkable is how little evidence there is that employers have actually requested or required applicants or employees to disclose this personal information as a condition of employment.").

[136]*See* Gaydos, *supra* note 9.

[137]Philip L. Gordon et al., Social Media Password Protection and Privacy—The Patchwork of State Laws and How It Affects Employers, 3–4, 11 (2013), http://www.littler.com/files/press/pdf/WPI-Social-Media-Password-Protection-Privacy-May-2013.pdf.

[138]Gaydos, *supra* note 9.

or that existing law already prohibits this activity.[139] As discussed in this part, some of these arguments simply fail; others, although credible, are ultimately not persuasive.

Although the statistics vary, obviously many employers rely upon on social networking sites, at least in part, to screen applicants.[140] However, users are increasingly relying upon privacy settings to limit the public's access to their social media profiles,[141] which means employers who seek publicly available social media information about those users may come up empty-handed. Asking for direct access in a job interview or from a current employee is a logical next step for employers seeking this type of information.[142] Indeed, deplorable though it may be, some employers have done just that, as made clear in the Introduction.[143] Although calling this practice a trend may be a stretch,[144] the likelihood that employers are currently or will begin to ask employees or job applicants for online account login information is significant enough that seventeen states have already passed legislation to curtail the practice and twenty-seven more have or are considering it. Moreover, a legislative body does not need a large number of examples of egregious behavior before it acts to prohibit it. Legislatures can—and do—anticipate problems and seek to prevent

---

[139]*See, e.g.*, Anita Ramasastry, *Can Employers Legally Ask for Your Facebook Password When You Apply for a Job?: Why Congress and the States Should Prohibit This Practice*, VERDICT: LEGAL ANALYSIS AND COMMENT. FROM JUSTIA (Mar. 27, 2012), http://verdict.justia.com/2012/03/27/can-employers-legally-ask-you-for-your-facebook-password-when-you-apply-for-a-job.

[140]*See Managing Your Online Image Across Social Networks*, *supra* note 5.

[141]*See* GORDON ET AL., *supra* note 137, at 2 ("[U]sers of social media increasingly are resorting to the privacy settings to screen their social media activity from others, including employers. According to one study, 15 percent of Facebook users (or nearly 150 million users), 7 percent of LinkedIn users (or nearly 15 million users), and 5 percent of Twitter users (or more than 27 million) modified privacy settings specifically with work in mind. These statistics do not encompass the tens of millions of other users who take advantage of privacy settings for other reasons.") (footnote omitted); MADDEN, *supra* note 6, at 7–8; *What Is the "Norm" for Privacy Settings on Social Networking Sites?*, *supra* note 6.

[142]*See* Bradley Shear, *SNOPA: A Privacy Win-Win for Social Media Age*, INNOVATION INSIGHTS (Feb. 19, 2013, 10:00 AM), http://insights.wired.com/profiles/blogs/right-to-digital-privacy-will-be-protected-by-the-social#axzz2WWHKcFsV ("Without the protections that [password protection legislation] provides, how long will it be before it becomes commonplace for employers to require job applicants and/or employees provide access to personal password protected digital accounts as part of the employment process?").

[143]*See supra* text accompanying notes 1–4.

[144]*See supra* text accompanying notes 8–9.

them before they escalate. Attorney Bradley Shear, a proponent of this legislation, has pointed to the Genetic Information Nondiscrimination Act of 2008 (GINA)[145] as one such example:

> GINA was not enacted because of a high profile incident where an employer required a candidate to submit his genetic information as part of the application process; it was enacted as a pre-emptive measure. In contrast, there are already multiple verifiable situations where employers are requiring job applicants provide their personal digital credentials as part of the application process.[146]

Given that employee privacy interests have become virtually nonexistent,[147] any attempt at increasing them should be encouraged.

At least one critic of this legislation has suggested that social media websites' Terms of Service (TOS) agreements will prevent employers from doing this because it violates TOS provisions.[148] For instance, the Facebook Statement of Rights and Responsibilities states that users "will not share your password . . . , let anyone else access your account, or do anything else that might jeopardize the security of your account."[149] LinkedIn contains a similar provision.[150] However, the TOS agreements are not legally binding on others, such as employers, who may not even be users of the site. As such, it is highly unlikely that social media websites' TOS will deter employers from this practice.

Some of the criticism leveled at the passage of this legislation ignores important characteristics of social media. For instance, consider the dramatic hand-wringing contained in the following report, written by attorney Philip Gordon, a frequent critic of this legislative trend:

> 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

---

[145]Pub. L. No. 110-233, 122 Stat. 881 (2008).

[146]Shear, *supra* note 142.

[147]*See supra* note 89.

[148]*See* Gaydos, *supra* note 9.

[149]*Statement of Rights and Responsibilities*, Facebook, https://www.facebook.com/legal/terms (last updated Nov. 15, 2013).

[150]*User Agreement* § 2.4, LinkedIn, http://www.linkedin.com/legal/user-agreement (last updated Mar. 26, 2014).

> restricted access social media account is private no matter how many people the user invites to view that content and regardless of the relationship between the user and the viewer. Put more plainly, these laws are based on the belief that, for example, a Facebook user who has more than 500 "Friends," including current and former supervisors and other executives at his current employer, can establish the "privacy" of his content by using Facebook's privacy settings to restrict access to "Friends Only."
>
> No court has ever construed the tort of invasion of privacy by intrusion upon seclusion so broadly. That tort requires a "private fact" which can be the subject of an intrusion. The vast majority of courts have held that, if the fact that is the subject of the claim has been disclosed to even a few people not under a legal or contractual obligation of confidentiality, the fact is not private and the intrusion upon seclusion claim fails. To be sure, a few cases have permitted an intrusion upon seclusion claim to proceed even though the plaintiff had shared the private fact with others. However, in virtually all of these cases, the private fact was shared within a group that had a specific relationship with the plaintiff, such as coworkers or co-participants in an *in vitro* fertilization program. We are not aware of any case holding that facts disclosed to dozens or hundreds of people who do not form a cohesive group are "private facts," especially when that group includes management-level employees of the employer who is the defendant on the privacy claim. In sum, the password protection laws create a "ring of privacy" with a circumference far larger than any court has recognized to date.[151]

As discussed previously, robust social media sites, such as Facebook or LinkedIn, often serve a variety of different functions, some of which allow users to post "private facts" that the law may protect—either through a private message sent to another user or by limiting which contacts may view posted content.[152] A person with access to the account may not necessarily know which areas are private and which are public until the private content has been seen. By then, the damage has been done. Thus, at least with regard to private messages exchanged via social media sites or posts with limited visibility, the password protection laws hardly create a new "ring of privacy" as Gordon claims. Instead, they simply recognize that new technology requires enhanced privacy legislation to ensure that existing privacy rights are appropriately recognized and protected.

Moreover, assuming this legislation does indeed create new privacy rights in personal online accounts, this is a suitable response to the demise

---

[151]Gordon et al., *supra* note 137, at 3–4 (footnotes omitted). This quote is taken from a subsection titled "How Social Media 'Password Protection' Legislation Radically Rewrites the Common Law of Privacy." *Id*.

[152]*See supra* note 94 and accompanying text; *see also Ehling II*, 961 F. Supp. 2d 659, 669 (D.N.J. 2013).

of employee privacy rights in recent years, especially regarding employees and applicants who attempt to preserve the privacy of their personal accounts. Gordon's argument ignores case law that indicates that some courts are ready to find privacy rights in the very type of social media content he addresses. *Ehling II* and *Crispin* in particular are such cases. Also, Determann and Sprague point out that *Stengart, Pure Power Boot Camp*, and *Pietrylo* "indicate a clear willingness on the part of the courts to consider e-mail and other types of electronic messages stored on personal web-based accounts to be within a zone in which employees have a reasonable expectation of privacy."[153] Thus far, however, these cases are few and far between. Given the snail's pace at which courts are addressing these issues, legislative response is entirely appropriate.

The final argument against the necessity for password protection legislation is that existing law, such as the National Labor Relations Act[154] (NLRA), common law privacy torts, and the SCA, may already prohibit employers from asking for personal online account access. Although the possible applicability of the SCA is an interesting suggestion, it, as well as the other existing laws upon which opponents rely, does not provide convincing support for the claim that password protection laws are unnecessary.

The NLRA and common law privacy claims might give employees some relief from privacy intrusions of the kind contemplated in this article. However, because the NLRA applies only to concerted activity,[155] it will not support employees or job applicants acting alone (which of course most do) who object to requests for online account password information. Regarding common law privacy claims, the most likely of which is intrusion into seclusion,[156] most courts have held that consent is a bar to this claim.[157] As explained in more detail later regarding the possible applicability of the SCA, although many scholars argue that valid employee

---

[153]Determann & Sprague, *supra* note 89, at 1009.

[154]Pub. L. No. 74-198, ch. 372, 49 Stat. 449 (codified as amended at 29 U.S.C. §§ 151–169 (2012)).

[155]29 U.S.C. § 157 (2012) ("Employees shall have the right to . . . engage in . . . concerted activities for the purpose of . . . mutual aid or protection. . . .").

[156]Note, *Negligent Hiring and the Information Age: How State Legislatures Can Save Employers from Inevitable Liability*, 53 Wm. & Mary L. Rev. 1397, 1416 (2012) ("Of the four common law invasion of privacy torts, most plaintiffs turn to intrusion upon seclusion to redress privacy violations in the employment context.").

[157]*See* 62A Am. Jur. 2d *Privacy* § 221 (Feb. 2014 update).

consent is suspect in the employment relationship, courts are still willing to find that consent bars a claim in SCA cases.[158] Just as the lack of consent will not be present in all SCA claims, the same is true here. Even more persuasively, employee plaintiffs have generally had little success in bringing tort claims for intrusion upon seclusion against employers. Indeed, many scholars have criticized the common law tort of invasion of privacy as being a woefully inadequate source of privacy protection, especially because courts often look to employer practices, rather than existing social norms, to determine whether particular behavior is reasonable.[159]

Finally, Gordon and other opponents of the legislation argue that the SCA, which makes it illegal to intentionally access electronic communications without authorization, already prevents employers from asking for login information to employees' or applicants' online accounts.[160] Of all the criticisms against this legislation, the argument that the SCA may already prohibit employers from accessing employees' or applicants' online accounts is the strongest, although it too is not persuasive enough to conclude that the legislation is unnecessary.

---

[158]*See infra* text accompanying notes 163–164; *cf.* Poore, *supra* note 8, at 514 ("The tort of intrusion upon seclusion involves a simple breach of privacy with no further dissemination required, but a social media site user's consent to be monitored or his or her voluntarily surrender [sic] of an account password would likely defeat any action under this tort, because the intrusion must be unauthorized to be actionable.").

[159]*See* Kim, *supra* note 89, at 908 ("Such an approach permits employers to destroy any expectations of privacy simply by announcing privacy-invading practices in advance, and regularly carrying them out. The common law privacy tort similarly turns on business practices, and courts have relied on the existence of a business justification to reduce an employee's expectation of privacy or render the intrusion inoffensive") (footnote omitted); *see also, e.g.*, Ciocchetti, *supra* note 17, at 300 (citing Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 665 (N.J. 2009)); Ronald P. Angerer II, *Moving Beyond a Brick and Mortar Understanding of State Action: The Case for a More Majestic State Action Doctrine to Protect Employee Privacy in the Workplace*, 4 Charlotte L. Rev. 1, 9–10 (2013).

[160]18 U.S.C. § 2701 (2012); *see* Philip Gordon, *New Jersey Court's Decision Provides Roadmap for Access to Employees' Restricted Social Media Content*, Publications: Littler Mendelson (Aug. 27, 2013), http://www.littler.com/publication-press/publication/new-jersey-court-access-employees-restricted-social-media; Rebekah Bradway, Social Media Password Privacy Legislation: The Trend, Utah's Law, and Whether It's Necessary 11 (Apr. 26, 2013) (unpublished manuscript), *available at* http://www.scribd.com/doc/138106188/Social-Media-Password-Privacy-Legislation (arguing that existing law, such as the SCA, make password protection laws "excessive"); Daniel I. Prywes & Jena M. Valdetero, *Proceed at Your Peril: Questions Abound with New State Laws Restricting Employer Access to Employees' Personal Social Media Accounts*, Bloomberg BNA (June 10, 2013), http://www.bna.com/new-state-laws-restricting-employer-access-to-employees-personal-social-media-accounts/; Ramasastry, *supra* note 139.

It is true that "courts have held that plaintiffs may maintain claims for violation of the SCA where employers accessed websites without authorization even though the websites were accessible to other parties."[161] In fact, the important decision in *Ehling II* held that the SCA applies to nonpublic Facebook posts:

> . . . Facebook wall posts that are configured to be private are, by definition, not accessible to the general public. The touchstone of the Electronic Communications Privacy Act is that it protects private information. The language of the statute makes clear that the statute's purpose is to protect information that the communicator took steps to keep private. Cases interpreting the SCA confirm that information is protectable as long as the communicator actively restricts the public from accessing the information.
>
> . . . The Court finds that, when users make their Facebook wall posts inaccessible to the general public, the wall posts are "configured to be private" for purposes of the SCA.[162]

After determining that the SCA is applicable to a particular private electronic message, the next step is to consider whether any exceptions apply, one of which is a requirement that the access to the communication be "unauthorized."[163] Indeed, the SCA cases that are applicable to the topic of this article all turn on the issue of whether the access was authorized. In *Ehling II*, after holding that the SCA applied to private social media wall posts, the court found that the employer had not violated the SCA because the person who accessed the account in question and provided information to the employer was one of the plaintiff's accepted contacts and was thus authorized to view and even make copies of the posts.[164] However, other cases have reached an opposite conclusion and found access to be unauthorized. In *Pure Power Boot Camp*, the court found that the employer violated the SCA by accessing the employee's personal e-mail account through the employee's saved username and password on the employer's computer.[165] The court in *Pietrylo v. Hillstone Restaurant Group* upheld the jury's determination that the employer violated the SCA by demanding a password from an employee to a private blog because the employee was

---

[161]Argento, *supra* note 90, at 236–37.

[162]*Ehling II*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013) (citations omitted).

[163]18 U.S.C. § 2701; *Ehling II*, 961 F. Supp. 2d at 669.

[164]*Ehling II*, 961 F. Supp. 2d at 669–70.

[165]Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 556 (S.D.N.Y. 2008).

essentially coerced into providing that information.[166] Finally, the Ninth Circuit Court of Appeals held in *Konop v. Hawaiian Airlines, Inc*. that the President of Hawaiian Airlines violated the SCA by using other users' passwords (even though given voluntarily) to access a private blog created by a Hawaiian Airlines pilot.[167]

While the previously mentioned cases are helpful and encouraging, the concept of valid employee consent is complex. Many scholars argue that an employee's consent to particular employer demands is often suspect. One commentator argues persuasively that requiring job applicants or employees to provide their user name or login information so that employers can access personal media accounts is inherently coercive, given the nature of the relationship between the two parties.[168] Willborn makes a similar argument, noting that the issue of consent in the privacy context "creates special problems in the workplace. Everyone agrees that consent is a difficult and compromised concept in employment law, although the reasons vary. . . . But the bottom line is the same: consent within the employment relationship is compromised and must be regarded with at least some skepticism."[169]

Certainly the possible applicability of the SCA should cause employers to consider carefully whether to seek access to an employee's online accounts (at least in those states in which the practice has not been prohibited). An employee who is faced with either termination or allowing an

---

[166]Pietrylo v. Hillstone Rest. Grp., No. 06–5754 (FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009).

[167]302 F.3d 868, 879–80 (9th Cir. 2002) (concluding the users who granted access had not actually used the site and therefore could not qualify as authorized users under the statute).

[168]Nicholas D. Beadle, Note, *A Risk Not Worth the Reward: The Stored Communications Act and Employers' Collection of Employees' and Job Applicant's Social Networking Passwords*, 1 Am. U. Bus. L. Rev. 397, 403 (2012) ("[E]mployees who disclose their passwords in this scenario do not so much choose to reveal them as they are compelled. Employers should know such disclosure is not voluntary; therefore, successful demands for employee passwords do not produce SCA authorization.") (footnote omitted). Beadle makes a similar argument regarding applicants. *Id*. at 403–04.

[169]Steven L. Willborn, *Consenting Employees: Workplace Privacy and the Role of Consent*, 66 La. L. Rev. 975, 976 (2006) (footnotes omitted); *see also* Chang, *supra* note 87, at 1 ("[W]ith unemployment close to 13 million people, many who obtain an interview may not be in a position to say no and walk away."); Roche, *supra* note 87, at 191; Valdes & McFarland, *supra* note 1 ("Lori Andrews, a law professor at IIT Chicago-Kent College of Law specializing in Internet privacy, is concerned about the pressure placed on applicants, even if they voluntarily provide access to social sites. 'Volunteering is coercion if you need a job,' Andrews said.").

employer to access her private information (or a job applicant looking for work) may very well have an argument that such a Hobson's choice is the type of coercion that the SCA prohibits. However, not all cases will involve coercion of the type that implicates violation of the SCA, regardless of how one feels about the issue of meaningful consent. As the Introduction to this article explains, at least one job applicant, Justin Bassett, refused to consent and walked away from the job.[170] Furthermore, although *Pietrylo* supports a conclusion that employees *may* be coerced into allowing access,[171] other cases support an opposite conclusion. "Because employees may be deemed to have consented to surveillance . . . the Act's protections have been found inapplicable in a number of workplace cases."[172] Thus, although it may be valid in some cases, a claim that access to an online account was unauthorized because the employee or applicant did not truly consent is not a reliable or consistent source of privacy protection.

The SCA is also an inadequate privacy safeguard because, as courts, scholars, and commentators agree, it is outdated, complicated, and confusing.[173] Its limitations regarding the technology to which it applies has

---

[170]*See supra* text accompanying note 1.

[171]*See supra* note 166 and accompanying text.

[172]Kim, *supra* note 89, at 914–15. Kim concludes that "[a]lthough the ECPA could be interpreted in ways more protective of employee privacy, under current interpretations it provides rather weak protection against employer scrutiny of employees' electronic communications." *Id*. at 915 (footnote omitted); *see also* Determann & Sprague, *supra* note 89, at 1001 ("Because of the exemptions contained in both the Wiretap Act and the SCA, commentators are in general agreement that the ECPA is ineffective in providing employees with any privacy protections relative to work-related e-mail messages and other forms of wire and electronic communications."); Poore, *supra* note 8, at 517 ("Although the *Pietrylo* court found that coerced consent is not authorization within the meaning of the SCA, other courts could rule the other way.").

[173]*See, e.g.* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (noting the ECPA "is ill-suited to address modern forms of communication"); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (stating the ECPA "is famous (if not infamous) for its lack of clarity"); Determann & Sprague, *supra* note 89, at 998–99 ("[A]pplying the ECPA has been wrought with difficulty, particularly for alleged violations arising from the workplace. . . . It has not been regarded as a model of statutory clarity."); Simon M. Baker, Seminar Article, *Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered Its Protections Obsolete*, 22 DePaul J. Art Tech. & Intell. Prop. L. 75, 109 (2011) ("[The SCA] is simply not designed to deal with modern technology."); Rudolph J. Burshnic, Note, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 Wash. & Lee L. Rev. 1259, 1264 (2012) ("The SCA is notoriously complicated and confusing, and its application to social networking sites has only

resulted in courts' increasing inability to apply it uniformly. Protection may also depend on where the communications are stored and whether they have been read by the recipient.[174] Medina notes, for example, that "the same email is subject to different protection depending on whether it is in transit, stored on a home computer, opened and stored in remote storage, unopened and stored in remote storage for 180 days or less, or unopened and stored in remote storage for more than 180 days."[175] Given that private messages sent between users on a social media website are similar to e-mail, not surprisingly, *Crispin* held that the SCA applies to them, depending upon whether they are read or unread.[176] Further, although *Ehling II* and *Crispin* both held that the SCA applies to content posted on a Facebook user's wall, in light of the current variation in SCA case law, these cases are certainly no guarantee that other courts will reach similar conclusions.[177]

Practical limitations also weaken the argument that the SCA prohibits employers from asking for online account passwords. Much of the social media access legislation extends beyond attempts to gain direct access by also prohibiting indirect access such as shoulder surfing or requiring the applicant or employee to change existing privacy settings so that the

---

further muddied the waters.") (footnote omitted); Lindsay S. Feuer, Note, *Who Is Poking Around Your Facebook Profile?: The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites*, 40 Hofstra L. Rev. 473, 502 (2011) (noting that, with respect to the SCA, "[s]everal courts have experienced difficulty in analyzing problems involving modern technology within the confines of the current statutory framework"); Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 Am. U. L. Rev. 267, 270 (2013) ("[D]iverging judicial interpretations regarding the SCA's applicability to modern technologies, such as Webmail, have created serious concerns as to the statute's continued viability. . . . These differing interpretations have created uncertainty regarding the scope of the SCA.") (footnote omitted).

[174]*See* Soma et al., *supra* note 86, at 520–21 (discussing different privacy protection under the SCA depending on whether a message is in transmission or storage); Arredondo-Santisteban, *supra* note 20, at 224–24.

[175]Medina, *supra* note 173, at 292.

[176]*See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal 2010); *supra* text accompanying note 104.

[177]State laws similar to the SCA are also unlikely to provide privacy protection to employees. *See* Kim, *supra* note 89, at 915 n.68 ("A number of states have enacted statutory protections analogous to the federal ECPA and in some cases, these statutes have narrower exceptions. Nevertheless, these state laws have generally not provided any significant protection in the employment context.").

information is publicly available.[178] Whether the SCA would prohibit either of those two actions is questionable. The SCA is also a cumbersome, inefficient method of protecting privacy rights and may not have a significant impact on employer behavior. Only the few employees who are negatively affected by such an intrusion will bring a case, and even those will take time to be resolved. "However, all employees . . . subjected to these intrusions have experienced an invasion of their right to information privacy."[179]

Clearly then, forcing employees to rely on existing law (to the extent that it is even applicable at all) to protect and enforce their privacy rights is not a fair or workable solution. Laws that may apply to one employee will simply not be applicable to others, leaving many victims without adequate recourse. Indeed, those existing laws certainly did not protect Robert Collins or Justin Bassett.[180] In the absence of coercion or evidence that private messages were read or unread, as is required to prove violation of the SCA, or the concerted activity required for the NLRA to apply, larger concerns related to employee privacy and dignity dictate that putting an employee in such a position should simply be off limits (within limited exceptions). An affirmative legislative statement of public policy regarding employee privacy rights is a far better alternative. Failure to do so sends an equally clear message that employee privacy rights are not important. "By finding that certain areas are worthy of protection, the law validates and reinforces claims of privacy; by declining to do so, the law negates those claims, further diminishing expectations of privacy."[181]

Lastly, this legislation is currently applicable to employers in seventeen states. Congress and twenty-seven other states have or are considering it. Should the trend continue, at least some of those states will enact some form of the legislation in the coming years. In those states, the question of whether existing law applies is less relevant. Of more relevancy are efforts to improve upon those statutes and legislative proposals so that they are meaningful and well balanced. To the extent that the legislation is here to stay, the Proposed Act in this article is useful.

---

[178]*See supra* text accompanying notes 55–57.

[179]Poore, *supra* note 8, at 518.

[180]*See supra* text accompanying notes 1–2.

[181]Kim, *supra* note 89, at 917.

At this point, it also bears mentioning that password legislation may *benefit* employers, at least according to some scholars and practitioners. Much has been written about the need for employers to take care when searching online for information about job applicants to avoid discovering details about the applicant's protected status.[182] This may be especially true if employers access private material posted on the applicant's social media profile. Statutes that limit access to personal online accounts ensure that employers do not unwittingly learn about protected information that the employee attempted to keep confidential. It may also protect employers from negligent hiring claims. Bradley Shear points out that Maryland's legislation may save Maryland businesses millions of dollars a year in costs to monitor their employees' personal digital accounts as well as in cyber liability insurance premiums that would accompany a duty to monitor employees in the digital and social media space.[183] He also concluded that because businesses will not have access to employees' digital content, they also will not be liable for it.[184]

Although this article advocates in favor of the need for online account password protection legislation, it shares some concerns regarding the statutory patchwork that multistate employers must negotiate, as well as

---

[182]*See, e.g.*, Chang, *supra* note 87, at 4 ("[U]sing social media to screen applicants carries considerable legal risks. For example, an employer could—even unknowingly—make a hiring decision based on an applicant's Title VII or ADA protected status. If a hiring manager searches an applicant's Facebook photos and sees her wedding pictures, the applicant's religion may be revealed. His alumni affiliation may reveal his age. . . . Our social networking activity holds a library of information."); Poore, *supra* note 8, at 519 ("Employers . . . who pry into the online activities of potential and current employees . . . might face unanticipated liability based upon adverse action they take in response to content they view on social media accounts. . . . Information that an employer . . . accesses on a social media site may reveal that an individual is a member of a protected group, based upon age, disability, marital status, religion, race, or national origin, for example."); Schess, *supra* note 91, at 447.

[183]Bradley Shear, *Maryland's Facebook Username and Password Law Is a Win for Employers, Employees, and Job Applicants*, Shear on Social Media Law (May 2, 2012) [hereinafter *Maryland's Facebook Username and Password Law Is a Win for Employers*], http://www.shearsocialmedia.com/2012/05/marylands-facebook-username-and.html. Shear has argued further that

> Protecting personal digital privacy will help grow the economy and foment new technological breakthroughs. If people believe their personal password protected digital thoughts, ideas, and creations are statutorily protected they will increase their usage of Dropbox, Microsoft SkyDrive, Google Plus, Facebook, etc. It is vital for our country's competitive future to implement public policy that encourages increased digital platform participation in our increasingly connected world.

Shear, *supra* note 142 (alteration omitted).

[184]Shear, *Maryland's Facebook Username and Password Law Is a Win for Employers, supra* note 183.

issues regarding particular provisions of individual pieces of legislation. The outcome of the present situation, in which the law differs considerably from state to state, is likely to cause confusion and administrative inefficiencies for employers, both within their own states and for those who manage employees elsewhere.[185] The varying definitions of important terms such as "social media" and "personal account" (or the lack of such definitions altogether), and the differences in scope regarding prohibited activity, the exceptions, and the available remedies, are also areas of concern. Additionally, many of the existing statutes and proposed bills are overbroad by giving the employer unlimited access to largely personal accounts that are used for only limited employment purposes. These issues lead to a conclusion that the uniformity available by adopting a model statute is desirable. The Proposed Act presented in this article, to which we now turn, addresses these issues. Further discussion about some of the major problems with existing legislation, as well as an explanation for how the Proposed Act addresses them, follow in Part III.B.

III. The Proposed Act—Striking the Proper Balance

While the state statutes are a good beginning toward recognizing legitimate privacy interests in employees' and applicants' online accounts, the many differences among the conflicting laws are a major problem. Moreover, many leave out important features while others are overbroad and weighted too heavily in favor of employers. Given that technology monitoring is an issue of national importance,[186] federal legislation is the best solution.[187] A federal statute is the most efficient and appropriate way to guarantee online employee privacy and ensure uniformity, resulting in a

[185]Gordon et al., *supra* note 137, at 11 ("As additional laws are considered and no doubt passed by other states, the potential for confusion and administrative difficulty will only increase.").

[186]Levinson, *supra* note 16, at 419–21.

[187]Even those generally opposed to the legislation agree that one federal law is preferable to the current system. *See, e.g.*, Gordon et al., *supra* note 137, at 13 ("[T]here does not appear to be any end in sight to the rash of legislation. As such, the only practical solution may be legislation at the federal level that will preempt all state legislation and common law tort claims . . . covering the subject matter to prevent the patchwork of state laws from becoming even more complex and even more unwieldy.").

proper balance of the interests involved, among states across the nation, and also between individual employers and employees.[188] Federal legislation will also benefit employers, especially those operating in several states, by easing the administrative burdens of developing and maintaining consistent policies, which will result in more employees being treated with dignity and fairness.[189] Particularly with regard to the flawed application of the SCA, a federal statute is desirable.[190] Even in the absence of federal legislation, those states currently considering enacting this type of legislation may benefit from the following Proposed Act and the discussion that follows.[191] It may also help state legislatures improve the statutes they have already enacted.[192]

A. The Employee Internet Privacy Protection Act

The proposal below, titled the "Employee Internet Privacy Protection Act," borrows from the best of the current statutes, proposed laws, and other suggestions regarding model privacy legislation. Sources and minor

---

[188]*Id.*; *see also*, Lipps, *supra* note 96, at 674 ("A federal statute would provide a clear indication from Congress of the importance of protecting electronic communication, and would not subject employers to a variety of state statutes and judicial interpretations."); Soma et al., *supra* note 86, at 527 ("Because the reach of e-messaging services erases state and national borders, any legislative action to further address and clarify e-message privacy interests must be undertaken at a federal level to be effective.") (footnote omitted) (internal quotation marks omitted); Poore, *supra* note 8, at 509 ("Federal legislation could provide a comprehensive set of protections with appropriate exceptions and resolve apparent conflicts between state laws and other federal laws in this subject area.").

[189]Levinson, *supra* note 16, at 421.

[190]*See, e.g.*, Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. Va. L. Rev. 461, 529 (2012) (arguing that a federal statute, replacing the ECPA, designed to regulate employee monitoring would be ideal because it would establish baseline protections for employees' right to privacy).

[191]Levinson, *supra* note 16, at 393 ("[A]n actual draft may be helpful in pushing legislatures to adopt real change. Providing a legislature with a draft rather than only ideas may result in a more receptive audience because a draft appears to provide a more definite course for reform and to be less onerous than starting from scratch. The legislature may have to assess every provision and may decide to change every one, but by providing a starting point, the process of beginning may be made easier.").

[192]Interview with Brian Cronin, former Idaho State Representative, in Boise, ID (Aug. 20, 2013) (stating that legislatures spend a lot of time in subsequent years revising statutes to clear up unintended problems).

explanations are annotated in footnotes within the Proposed Act itself. Part III.B addresses the important considerations underlying the chosen language.

I. Definitions
   A. Employer—a public or nonpublic entity, an individual engaged in a business, or any other person or organization that obtains the services of individuals in exchange for financial remuneration. Employer shall also include any agent, representative, or designee of such an employer.[193]
   B. Employee—any person who works, including part time, for an employer in exchange for financial remuneration. Employee includes an independent contractor.[194]
   C. Personal online account or service—any collection of electronically stored information, including, but not limited to, such collections stored on social media Internet web sites, in electronic mail, and on electronic devices, which are opened, used, or maintained by any employee or applicant primarily for personal communications unrelated to the employer's business purposes.[195]

---

[193]This provision draws from L.B. 58, 103d Leg., 1st Sess. (Neb. 2013) ("Employer means a public or nonpublic entity or an individual engaged in a business, an industry, a profession, a trade, or other enterprise in the state, including any agent, representative, or designee of such an employer.") and the Model Electronic Privacy Act, § 1(c), *Legislative Briefing Kit on Electronic Monitoring*, ACLU (Mar. 11, 2001), https://www.aclu.org/technology-and-liberty/legislative-briefing-kit-electronic-monitoring (defining an employer as "any person, partnership, corporation, or other organization engaged in commerce, or any other person or organization which obtains the services of individuals in exchange for financial remuneration").

[194]Model Electronic Privacy Act, *supra* note 193, § 1(b) ("[T]he term 'employee' means any person who performs services for an employer in exchange for financial remuneration, including part time, leased, or former employees."); Levinson, *supra* note 16, at 395 ("Employee means any person who works, including part-time, for an employer 'in exchange for financial remuneration.'") (quoting Model Electronic Privacy Act *supra* note 193, § 1(b)); L.B. 1194, 2013 Leg., 1st Reg. Sess. (Me. 2013) ("'Employee' means a person who is permitted, required or directed by an employer to engage in employment for consideration of direct or indirect gain or profit. 'Employee' includes an independent contractor.").

[195]*See* Utah Code Ann. § 34-48-102(4)(a) (West 2013) ("Personal internet account means an online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer."); H.B. 1407, 2014 Leg., Reg. Sess., (N.H. 2014) ("Personal account means an account, service, or profile on a social networking website that is used by a current or prospective employee primarily for personal communications unrelated to any business purposes of the employer.").

II. Prohibited Acts. An employer shall not:
  A. Suggest, request, require, or cause an employee or applicant for employment to do any of the following:
    1. Grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal online account or service;[196]
    2. Add any person, including the employer or his or her agent, to the employee's or applicant's list of contacts associated with a personal online account;[197]
    3. Divulge any information or content from an employee's or applicant's personal online account;[198] or
    4. Change or alter the privacy settings associated with the employee's or applicant's personal online account to affect a third party's ability to view the contents of the account.[199]
  B. Discharge, discipline, fail to hire, or otherwise penalize an employee or applicant for asserting his or her rights under this statute, assisting other employees in asserting their rights, reporting violations of this statute, or participating in enforcement actions under this statute.[200]
III. Exceptions. Nothing in this Act shall prohibit an employer from:
  A. Requesting or requiring an employee to allow observation of content from his or her personal online account

---

[196]This language comes directly from MICH. COMP. LAWS ANN. § 37.273(a) (West 2012). It prohibits both direct and indirect access in one clear section.

[197]*See* ARK. CODE ANN. § 11-2-124(b)(1)(B) (West 2013) ("An employer shall not require, request, suggest, or cause a current or prospective employee to. . . [a]dd an employee, supervisor, or administrator to the list or contacts associated with his or her social media account. . . ."); COLO. REV. STAT. ANN. § 8-2-127(2)(a) West (2013); OR. REV. STAT. § 659A.330(1)(b) (West 2014); WASH. REV. CODE ANN. § 49.44.200(1)(c) (West 2013).

[198]*See* CAL. LAB. CODE § 980(b)(3) (West 2013).

[199]*See* WASH. REV. CODE ANN. § 49.44.200(1)(d) ("An employer may not . . . [r]equest, require, or cause an employee or applicant 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. . . ."); *see also* ARK. CODE ANN. § 11-2-124(b)(1)(C); COLO. REV. STAT. ANN. § 8-2-127(2)(a).

[200]This borrows from both MICH. COMP. LAWS ANN. § 37.273(b) and the Model Privacy Act, *supra* note 193, § 7.

as cooperation in the employer's work-related investigation if:[201]

1. The employer is conducting a formal investigation, based upon receipt of reliable and reasonable information regarding employee misconduct, and requires observation of this content to ensure compliance with the employer's written employment policies;[202] and
2. The observation of such content is reasonably necessary to make a factual determination in the course of conducting a reasonable investigation; and
3. The employer does not request, require, suggest, or cause the employee to grant access to or disclose information that allows access to the employee's or applicant's personal online account or service.[203]
4. An employer exercising its rights under the immediately preceding subdivisions of this section shall use any information obtained through observation of the employee's personal online account only for the purpose of the formal investigation or a related proceeding.[204]

---

[201]This provision allows only for observation of particular content, borrowing from the concepts found in the Oregon and Washington statutes that do not allow direct access via login information. *See* Or. Rev. Stat. § 659A.330(4); Wash. Rev. Code Ann. § 49.44.200(2).

[202]This section builds on the concept found in the Colorado and Utah statutes that allows for certain exceptions based upon receipt of information regarding misconduct or violation of the law. *See* Colo. Rev. Stat. Ann. §§ 8-2-127(4)(a) and (b); Utah Code Ann. §§ 34-48-202(1)(c)(i) and (ii) (West 2013) (providing that an employer is not prohibited from conducting an investigation if there is "specific information" indicating it is necessary to ensure compliance with the law or that there has been an unauthorized transfer of proprietary, confidential, or financial information to the employee's personal Internet account).

[203]Or. Rev. Stat. § 659A.330(4) ("Nothing in this section prevents an employer from . . . [c]onducting an investigation, without requiring an employee to provide a user name and password, password or other means of authentication that provides access to a personal social media account of the employee. . . ."); Wash. Rev. Code Ann. § 49.44.200(2)(d) ("This section does not apply to an employer's request or requirement that an employee share content from his or her personal social networking account if the . . . employer does not request or require the employee to provide his or her login information.").

[204]This borrows language from Cal. Lab. Code § 980(c) (West 2013) (providing "that the social media is used solely for purposes of that investigation or a related proceedings") and Ark. Code Ann. § 11-2-124(e)(2)(B) ("If the employer exercises its rights under . . . this section, the

B. Requiring or requesting an employee to disclose a username, password, or other method of accessing an online account or service that is:
   1. Provided by the employer; or
   2. Set up by the employee at the employer's request; or
   3. Obtained by virtue of the employee's employment relationship with the employer;[205] or
   4. Used primarily for the employer's business purposes.

C. Requiring or requesting an employee to disclose a username, password, or other method of accessing an employer-issued or employer-owned, in whole or in part, electronic device.[206]

D. Obtaining information about an applicant or employee that is available in the public domain.[207]

IV. Waiver of Rights

A. The rights provided by this Act may not be waived, by contract or otherwise.[208]

V. Enforcement and Remedies

A. An employee or applicant who is injured by a violation of this Act may file a claim with the Department of Labor or bring a civil action against the employer in a court of competent jurisdiction.[209]

---

employee's username and password shall only be used for the purpose of the formal investigation or a related proceeding.").

[205]*See* COLO. REV. STAT. ANN. § 8-2-127(2)(b) ("[T]his subsection (2) does not prohibit an employer from requiring an employee to disclose any user name, password, or other means for accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems."); *see also* 820 ILL. COMP. STAT. ANN. 55/10(b)(2)(B) (West 2012); N.M. STAT. ANN. § 50-4-34(B)(2) (West 2013).

[206]*See* CAL. LAB. CODE § 980(d).

[207]*See* 820 ILL. COMP. STAT. ANN. 55/10(b)(3); OR. REV. STAT. § 659A.330(5).

[208]*See* N.J. STAT. ANN. § 34:6B-7 (West 2013) ("No employer shall require an individual to waive or limit any protection granted under this act as a condition of applying for or receiving an offer of employment. An agreement to waive any right or protection under this Act is against the public policy of this State and is void and unenforceable."); Model Privacy Act *supra* note 193, § 9; Levinson, *supra* note 16, at 418.

[209]*See* Levinson, *supra* note 16, at 416.

B. An employer who violates any provision of this act may be assessed a civil penalty in an amount not to exceed $1,000 for the first violation and up to $5,000 for each subsequent violation.[210]
C. In an action brought under this statute, if the court finds a violation of this chapter, in addition to assessing a civil penalty as set forth in Section V.B., the court may also award the prevailing employee or applicant reasonable attorney fees and costs, actual damages, and injunctive or other equitable relief, including mitigation or removal of any discipline imposed, reinstatement, promotion, back pay, and lost benefits.[211]

B. Proposed Act Discussion

Section (I)—Definitions. The Proposed Act broadly defines the terms employer and employee to cover both private and public employers, the employer's agents or representatives, and full- or part-time employees. It also extends to independent contractors. "[T]he rationale of the broad definition is that no employer is too small to take adequate protections to safeguard its employees' privacy."[212] Similarly, any person who works for another, whether as an employee or an independent contractor, has privacy interests that should be recognized.[213]

One major concern raised by the different statutes relates to the accounts or devices that the statutes cover. Many are simply too vague because they apply to "social media" and yet fail to define the term.[214] Others, such as California, define "social media" too broadly,[215] and the

---

[210]*See* Colo. Rev. Stat. Ann. § 8-2-127(5); N.J. Stat. Ann. § 34:6B-9 (providing up to $2,500 for subsequent violations).

[211]*See* Levinson, *supra* note 16, at 416.

[212]*Id.* at 423.

[213]The proposal does not define obvious terms such as "job applicant."

[214]For instance, both the Colorado and Maryland statutes apply to social media accounts, yet neither define the term.

[215]Cal. Lab. Code § 980(a) (West 2013) ("As used in this chapter, "social media" means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."); *see also* Eric Goldman, *Big Problems in California's New Law Restricting Employers' Access to Employees' Online Accounts*, Forbes (Sept.

Illinois statute inexplicably excludes e-mail from the reach of the law.[216] A few states differentiate between "personal" accounts, which are off limits to employers, and "nonpersonal accounts" which are not, yet some fail to define those terms or otherwise explain how a personal account differs from a nonpersonal one.[217] Others provide a definition that lacks logic or consistency[218] or that is so narrow that it essentially loses all meaning. For example, the Utah statute defines a "personal internet account" as one that an applicant or employee uses "*exclusively* for personal communications unrelated to *any* business purpose of the employer."[219] The following section excludes from the definition "an account created, maintained, used, or accessed by an employee or applicant for business related communications or for a business purpose of the employer."[220] These provisions fail to consider the fact that many social media accounts serve a dual purpose, both personal and professional, and thus give far too much deference to the employer by arguably allowing the employer access to an employee's personal Internet account if the employee makes even one reference about or on behalf of her employer. Professor Eric Goldman, for

---

28, 2012, 12:39 PM), http://www.forbes.com/sites/ericgoldman/2012/09/28/big-problems-in-californias-new-law-restricting-employers-access-to-employees-online-accounts/ ("[T]he law governs effectively all digital content and activity, both on the Internet and stored in local storage devices, not just social media. After all, what digital resource isn't 'an electronic service or account, or electronic content'? The coverage of the law has focused only on its application to social media accounts, but the law's unexpectedly broad reach—including to locally-stored content—virtually ensures that the law will have unintended consequences.").

[216]820 Ill. Comp. Stat. Ann. 55/10(b)(4) (West 2012) ("'Social networking website' shall not include electronic mail."). Several proposed bills also exclude email. *See, e.g.*, Minnesota (H.F. 2963, 87th Sess. (Minn. 2012)); Mississippi (H.B. 165, Reg. Sess. (Miss. 2013)); Missouri (H.B.286, 97th Gen. Assemb., 1st Reg. Sess. (Mo. 2013)); Nebraska (L.B. 58, 103d Leg., 1st Sess. (Neb. 2013)); North Dakota (H.B. 1455, 63d Leg. Assemb. (N.D. 2013)); South Carolina (H. B. 5105, 119th Sess. (S.C. 2012)).

[217]*See supra* text preceding and accompanying note 52.

[218]For example, in the provision defining "social media account," the Rhode Island statute states that it "does not include an account opened at an employer's behest, or provided by an employer, or intended to be used primarily on behalf of the employer"—as though such an account is somehow not a "social media account." *See* 2014 R.I. Pub. Law S2095A (to be codified at R.I. Gen. Laws Ann. § 28-56-1(1) (West 2014) (effective June 30, 2014). *See also* L.B. 1194 2013 Leg., 1st Reg. Sess. (Me. 2013). If the Rhode Island and Maine legislatures do not want social media accounts used for employment purposes to be covered by the acts, they would be better off simply excluding such accounts from their purview.

[219]Utah Code Ann. § 34-48-102(4)(a) (West 2013) (emphasis added).

[220]*Id*. § 34-48-102(4)(b).

example, criticizes California's statute for applying to personal social media without defining when a social media account is "personal."[221] He argues that while the law considers social media to be in only two states—personal or nonpersonal—social media accounts fit along a continuum with those two states as the end points.[222] In reality, "employers and employees routinely disagree about whether or not a social media account was personal or business-related."[223]

The Proposed Act clears up the conceptual difficulty regarding what type of accounts are covered with one comprehensive provision that clearly defines a "personal online account" and specifies what is meant by the word "personal." Although it borrows language from the Utah statute, it removes the implication that a personal account is only one that is unrelated to *any* business purpose of the employer and substitutes that with language from the New Hampshire bill, which prohibits attempted access to accounts that are used "primarily" for personal communications.[224] This definition is reflective of the continuum of online account ownership that Professor Goldman expressed above. It could also be instructive to courts that wrestle with the increasing number of employment cases regarding the "ownership" of social media accounts.[225]

The "online account or service" portion of the phrase was defined as broadly as possible to avoid becoming obsolete as technology changes. Although provisions regarding an employer's access to accounts in which it has a legitimate interest are found in myriad places within the statutes and proposed bills, it is most appropriately placed as an exception to

---

[221]Goldman, *supra* note 215.

[222]*Id.*

[223]*Id.; see supra* text accompanying notes 122–129; *see also* Scott A. Schaefers, *Oregon the Latest State to Pass Social Networking Privacy Legislation; Vermont Establishes Committee to Study and Recommend Such Legislation*, Trading Secrets (June 7, 2013), http://www.tradesecretslaw.com/2013/06/articles/legislation-2/oregon-the-latest-state-to-pass-social-networking-privacy-legislation-vermont-establishes-committee-to-study-and-recommend-such-legislation/ ("The Oregon law does not define 'personal' accounts, or on the flip side, those which are 'provided by, or on behalf of, the employer, or to be used on behalf of the employer.'"); Torphy-Donzella, *supra* note 9, ("[W]hile [Maryland's] law quite reasonably does not constrain an employer from demanding pass codes to 'non-personal' sites and devices, it does not provide any definition of what would be 'personal' as opposed to 'business.'").

[224]H.B. 1407, 2014 Leg., Reg. Sess., (N.H. 2014).

[225]*See supra* text accompanying notes 122–130.

prohibited acts. Thus, it is placed there in the Proposed Act and is addressed in more detail below—when discussing Exceptions.

The Proposed Act intentionally steers away from a focus on electronic devices, which is both misleading and unnecessary. Those statutes that apply specifically to the employee's or applicant's device may unwittingly provide a loophole for employers to avoid violating the law by simply asking the employee or applicant to open an account on an employer-owned device.[226] Moreover, the intent behind this legislation is to protect personal employee communications and content posted to and through their online accounts, not the means of access to those accounts. Thus, it is fitting that those accounts are the focus of the legislation that is intended to protect them.

Section (II)—Prohibited Acts. The specific language in the proposal's Prohibited Acts section is simple in form and yet comprehensive, thus resolving the confusion caused by the multitude of prohibited acts and their inconsistent treatment in the various statutes. The point of this legislation is to prohibit access to private material, so the language should be comprehensive enough to prohibit this in any form and by any method.[227] The employer may not ask for direct access through a username and password or indirect access through shoulder surfing, require the employee to "friend" the employer or the employer's representative,[228] or change privacy settings so that private content becomes visible to the

---

[226]For instance, the Colorado law prohibits the employer from requiring disclosure of "any user name, password, or other means for accessing the employee's or applicant's personal account or service *through the employee's or applicant's personal electronic communications device*." COLO. REV. STAT. ANN. § 8-2-127(2)(a) (West 2013) (emphasis added). The inclusion of this language could suggest that the employer is not prohibited from asking for password information for the employee's personal accounts that may, of course, be accessed from the employer's own computer.

[227]*See* Buckley, *supra* note 19, at 887–88 ("The reality is that the undesired conduct at issue . . . may be achieved through multiple techniques. Any attempt to eradicate the undesired conduct must effectively deter all method of engaging in such conduct. An employer may request a password so that he can access password-protected material, or he may instead 'shoulder surf' so as to escape liability under poorly crafted legislation. In order to unequivocally proscribe all methods of accessing password-protected material, Congress must prohibit demands for passwords, as well as demands for individuals to access private material in the presence of those who are prohibited from viewing it.").

[228]In their discussion of the survey that is the topic of their article, Abril et al. suggest that many employees believe it can be appropriate to "blend worlds" by inviting employers or supervisors to become a contact on a social networking website. Abril et al., *supra* note 82, at 102. This may be true in many instances, and, indeed, is not prohibited by this proposal

public. Retaliation language is similarly straightforward and broad "to encourage employees to advocate for and enforce their rights to privacy."[229]

The Proposed Act intentionally excludes language that prohibits employers from asking applicants or employees whether they have social media accounts. Such a prohibition is overbroad and could, for example, exclude employers who are seeking to hire a social media-marketing specialist from asking about their previous experience with social media accounts.[230]

Section (III)—Exceptions. Practitioners who represent employers appear to be most pleased by those state statutes that contain robust exceptions.[231] These lawyers object to the lack of exceptions contained in some of the legislation, or argue that the exceptions that do exist are too narrow and do not allow employers to investigate workplace misconduct such as harassment, misuse of employer-owned equipment, or misappropriation of trade secrets.[232] Admittedly, cases will arise in which an

---

because it limits only the *employer* from making the request, out of respect for the employee's privacy interests. An employee who wishes to forgo some of that privacy may make the request of the employer.

[229]Levinson, *supra* note 16, at 429.

[230]New Jersey Governor Chris Christie initially vetoed the bill in New Jersey in part because of such a provision. Letter from N.J. Governor Chris Christi to the New Jersey General Assembly (May 6, 2013), *available at* http://www.njleg.state.nj.us/2012/Bills/A3000/2878_V2.HTM ("Unfortunately, this bill paints with too broad a brush. For example, under this bill, an employer interviewing a candidate for a marketing job would be prohibited from asking about the candidate's use of social networking so as to gauge the candidate's technological skills and media savvy. Such a relevant and innocuous inquiry would, under this bill, subject an employer to protracted litigation, compensatory damages, and attorneys' fees—a result that could not have been the sponsors' intent.").

[231]*See, e.g.*, Philip L. Gordon & Lauren Woon, Re-Thinking and Rejecting Social Media "Password Protection" Legislation, Workplace Privacy Couns. (July 10, 2012), http://www.littler.com/2012/07/articles/state-law-claims/re-thinking-and-rejecting-social-media-password-protection-legislation (criticizing some of the legislation's exceptions as being "unjustifiably narrow").

[232]*See, e.g.*, Beth Zoller, Legislatures Aim to Protect Social Media Privacy of Employees and Applicants, Xpert HR.com (July 10, 2012), http://www.xperthr.com/news/legislatures-aim-to-protect-social-media-privacy-of-employees-and-applicants/7458/; Gordon, *supra* note 9 ("The absence of any exceptions to the general prohibition in the Illinois bill highlights another challenge for employers raised by this new genre of workplace regulation. The Maryland law contains exceptions for investigations of suspected securities fraud violations and suspected misappropriation of trade secrets. While these exceptions themselves are overly narrow, their

employer has a legitimate business reason for viewing an employee's private account.[233] Employers have a legitimate interest in their reputations, and in running a safe and efficient operation, as well as knowing the background and public profiles of employees and job applicants as that information relates to the employee's or applicant's ability to perform the job. Thus, some exceptions are indeed necessary, if for no other reason than a provision that includes exceptions will make clear that any other activity, besides that provided in the statute, is not allowed.

The Proposed Act provides an exception to allow employers to conduct reasonable, formal investigations into workplace misconduct. This allows employers to investigate workplace issues such as claims of harassment and bullying.[234] However, this exception extends only to the sharing of relevant content, similar to the Oregon and Washington statutes,[235] rather than allowing the employer to ask for login information, which presumably may be used outside of the employee's or applicant's presence. Thus, this exception would allow an employer to conduct a valid investigation into employee misconduct by taking a quick look into certain areas of the employee's personal online account, in the employee's presence, for reasonable investigative purposes only, without necessarily giving the employer carte blanche access to all of the content on the profile. The Proposed Act requires that any information upon which the employer bases a request to view content of an employee's or applicant's personal online account must be reasonably true and reliable. This language best balances the employer's legitimate interests and the employee's privacy (and the privacy of those with whom the employee has interacted on the social networking site). Lastly, employers retain the right to access any

---

absence from the Illinois bill suggests that the states are beginning to weave yet another inconsistent patchwork of laws that will further complicate for employers the already daunting challenge of regulating new technology in the workplace.").

[233]*See* Poore, *supra* note 8, at 508 ("While employers . . . have valid interests in monitoring users on their own networks for reasons related to security, productivity, protecting confidential and proprietary information, and protecting their reputations and brands, the legislation can carve exceptions for such monitoring, and at the same time, shield off-duty social media activity and protected social media communications in the workplace . . . setting from invasions of privacy.") (footnote omitted).

[234]*See* Gordon et al., *supra* note 137, at 11–12.

[235]Or. Rev. Stat. § 659A.330(4) (West 2014); Wash. Rev. Code Ann. § 49.44.200(2) (West 2013).

material available in the public domain. Although this language is unnecessary, as courts across the country have almost universally ruled that there is no right to privacy associated with material individuals post for public viewing on the Internet, enough states have included this language in their individual statutes that its inclusion is likely to be helpful to employers as they work to determine permissible boundaries.[236]

The statutes and bills contain many exceptions that were intentionally left out of the Proposed Act. Those exceptions that allow employers to access personal accounts to look for unauthorized downloading of confidential or proprietary information or securities laws violations are unnecessary, as is an exemption for law enforcement employers. Employers already have available safety mechanisms and procedures upon which they can rely if they believe these violations are occurring.[237] For example, the broad exceptions contained in the proposed federal Password Protection Act, which exempt government employees and any employees who work

---

[236]However, this does not necessarily mean that the practice of doing Internet searches on job applicants or current employees is wise. *See, e.g.*, Jacobs, *supra* note 7 ("While the potential upside of social media screening is the ability to obtain potentially valuable information showing the applicant to not be a desirable candidate for a position, one potential downside is that the employer may unwittingly gain knowledge of protected-class-status information, such as the religion, age, marital or pregnancy status, or sexual orientation of an applicant. . . . Thus, it may be better to rely on objective qualifications and engaging in personal interaction and assessment rather than to cast a wide net in terms of information gathering in the hopes of unearthing a single, perhaps salacious, disqualifying trait.").

[237]*See* AP, *Bill Would Allow Bosses to Seek Facebook Passwords*, CBS Charlotte (Apr. 3, 2013, 2:12 PM), http://charlotte.cbslocal.com/2013/04/03/bill-would-allow-bosses-to-seek-facebook-passwords/ ("University of Washington law professor Ryan Calo, who studies emerging technologies, said companies have federal, state and common laws that protect proprietary information. 'At first blush, it looks pretty common sense. If you're trying to investigate what happened and you suspect one of your employees, it seems like common sense you should be able to do this, however, there are legal mechanisms,' he said."); Lynne Bernabei & Alan R. Kabat, *Invasions of Privacy*, Nat'l L.J. (July 23, 2013), *available at* http://bernabeipllc.com/wp-content/uploads/Bernabei-Kabat-July-23-2012-National-Law-Journal.pdf ("Delaware's proposed legislation exempts law enforcement agencies—precisely the employment sector that motivated Maryland's legislation. It also proposes to exempt 'employers in the financial services industry' . . . . This loophole is big enough to drive a truck through, since the financial sector is one of the largest employers in Delaware, and almost anything can be an 'internal investigation.'"); Rebecca Herold, *Good Intentions Often Lead to Bad Privacy Results*, Privacy Professor Blog (Apr. 29, 2013, 9:31 PM), http://privacyguidance.com/blog/good-intentions-often-lead-to-bad-privacy-results/ ("There are already ways to investigate insider trading, as well as other types of insider fraud, which could be occurring within personal accounts. You get a warrant for that, or take other appropriate actions.").

with children under age thirteen,[238] are also unnecessary and, as such, simply unacceptable. As ACLU Legislative Counsel Chris Calabrese states, "These sections authorize sweeping and unnecessary fishing expeditions. There are already a broad range of tools for investigating misconduct. . . . Just because you work for the government or with children, you shouldn't forfeit the right to a private life online."[239]

Section (IV)—Waiver of Rights. Generally, because the employee-employer relationship is contractual, rights can be waived unless otherwise prohibited by law.[240] For instance, waivers have been found to be generally enforceable in separation and arbitration agreements,[241] in the absence of statutory language that expressly prohibits such a waiver.[242] Accordingly, a statute that grants employees specific rights regarding the privacy of their personal online accounts, without inclusion of an antiwaiver provision, runs the risk of being essentially meaningless if employers are free to request a waiver of rights under this law as a condition of employment. Thus, this provision is an important section of the Proposed Act.

---

[238]H.R. 2077, § (2)(d)(2)(B)(iii), S. 1426, § (2)(d)(2)(B)(iii), 113th Cong. (2013).

[239]Chris Calabrese, *Password Protection Act of 2012: A Good Start Against Employer Snooping*, ACLU Free Future Blog (May 9, 2012, 6:06 PM), http://www.aclu.org/blog/technology-and-liberty/password-protection-act-2012-good-start-against-employer-snooping; *see also* Bernabei & Kabat, *supra* note 237 ("The federal Password Protection Act of 2012 would allow executive-branch agencies to exempt positions 'requiring eligibility for access to classified information.' Since more than 4.2 million federal employees and contractors have security clearances, this means that numerous individuals could be required to disclose their private information in order to keep their jobs.").

[240]*See* Eve I. Klein et al., *Navigating the Murky Waters of Employment Waivers and Releases*, 82 N.Y. St. B. Ass'n J., no. 2, 2010, at 32.

[241]*See, e.g.*, EEOC v. SunDance Rehabilitation Corp., 466 F.3d 490, 499 (6th Cir. 2006) ("This court has upheld employees' waivers of claims under ADEA, EPA, and Title VII where the waiver was executed voluntarily and intelligently."); *see also* AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740 (2011) (upholding validity of arbitration agreement waiving customers' rights to participate in class action lawsuits); D.R. Horton, Inc. v. NLRB, 737 F.3d 344 (5th Cir. 2013) (upholding validity of arbitration agreement waiving employees rights to participate in collective employment-related claims).

[242]*See D.R. Horton, Inc*., 737 F.3d at 360 (noting the Federal Arbitration Act (FAA) "establishes a liberal federal policy favoring arbitration agreements" unless the "FAA's mandate has been overridden by a contrary congressional command") (internal quotation marks omitted.).

Section (V)—Remedies. Lastly, the Proposed Act addresses the diverse remedies from state to state, which to some are particularly troublesome.[243] The Proposed Act provides for a civil remedy since, at its essence, violation of this act is an invasion of privacy, which is typically remedied through a civil rather than criminal action. Making an offense of the statute a criminal act as well as imposing civil penalties seems both unnecessary and contrary to other statutes regarding employment law.[244] A private cause of action is desirable,[245] but the Proposed Act also delegates some possible responsibility to an administrative agency, as well as the courts, to allow the agency to proactively educate and enforce the law, reduce financial costs to the parties, and permit "decision makers with expertise in the area to be involved."[246] The penalty provision of the Proposed Act reflects an attempt to impose a penalty that is strong enough to have real impact without being punitive. Weak civil penalties, such as

---

[243]Bernabei & Kabat, *supra* note 237 ("The bad news is that these legislative efforts have a hodgepodge of enforcement mechanisms. For example, there are five bills pending in New York, two of which have both civil and administrative remedies, one of which has an administrative remedy alone and two of which have no statutory remedies. Michigan's and Washington's bills provide for a civil action for legal and equitable remedies; Michigan's also would create a misdemeanor offense punishable by up to 93 days in jail. New Jersey's and Ohio's bills provide both administrative enforcement and a civil action. Delaware and Illinois drafted their legislation as part of pre-existing statutes with enforcement mechanisms through both a state agency and a civil action.").

[244]For instance, common law privacy violations are torts rather than crimes. Moreover, most employment discrimination statutes result in civil rather than criminal penalties. Violation of this law should be no different.

[245]*See* Levinson, *supra* note 16, at 416, n.490 ("[W]ithout a private cause of action, 'there is likely to be significant underenforcement of privacy interests.'") (quoting Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 925–26 (2009)).

[246]*Id.* at 429. Regarding the proposed federal "Privacy Protection in Employment Act" that is the subject of her article, Levinson suggests,

> [T]he DOL is most likely to use an enforcement mechanism that is well suited to protecting employees' right to privacy. The agency already has in place mechanisms to provide compliance guidance, opinion letters, recommendations as to resolving disputes, and adjudicatory administrative hearings. While filing a claim with the DOL permits an employee a low cost means to settle a dispute, filing with the DOL is not generally a prerequisite to filing in court. Thus, employees are provided the option of a court suit rather than agency dispute resolution should they so prefer.

Id. at 430.

those in the Utah and Washington statutes, which impose only civil penalties of up to $500,[247] are unlikely to have the desired deterrent effect. On the other hand, the $10,000 penalty contemplated in SNOPA[248] may strike many as being too punitive, especially for a first offense. The proposal strikes a balance between those two approaches, imposing a fine of $1,000 for the first offense and allowing the court or administrative agency to impose a higher fine of up to $5,000 for subsequent violations. It gives the court discretion to award attorneys' fees and costs as well as actual damages and injunctive relief as may be shown and warranted.

The Proposed Act deliberately omits other miscellaneous provisions found in several of the laws and bills. Some statutory language, such as that found in the Michigan and Utah statutes, specifically provides that the law "does not prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring . . . ."[249] This provision is unnecessary—the intent of these statutes is primarily employee protection of private information, not to impact on an employer's obligation to make reasonable hiring decisions. These same two statutes state specifically that they are not intended to create a duty for an employer "to search or monitor the activity of a personal internet account"[250] or that an employer will not be liable for failing to request or require an employee or applicant for access to a social media account.[251] In other words, these laws inexplicably state that the employer has no duty to engage in behavior that is already prohibited by the statute and then absolve employers from liability for abiding by the law. These provisions are nonsensical. If the law specifically *prohibits* an employer from accessing an employee's or applicant's online account, there is certainly no need to state elsewhere that the employer has no duty to do so.

---

[247]Utah Code Ann. § 34-48-301(2) (West 2013); Wash. Rev. Code Ann. § 49.44.205(1) (West 2013).

[248]Social Network Online Protection Act, H.R. 537, § (2)(b)(1)(A), 113th Cong. (2013).

[249]Mich. Comp. Laws Ann. § 37.275(2) (West 2012); Utah Code Ann. § 34-48-202(3) (West 2013).

[250]Mich. Comp. Laws Ann. § 37.277(1); Utah Code Ann. § 34-48-203(1).

[251]Mich. Comp. Laws Ann. § 37.277(2); Utah Code Ann. § 34-48-203(2).

Conclusion

In less than three years, forty-four states have enacted or considered legislation that increases employee and job candidate privacy rights by limiting employer access to their personal online information. In this technological world, where employee privacy rights are, at least according to some, nonexistent, this legislative move toward restoring some of these rights is definitely a step in the right direction. However, current legislative attempts fall short of a fair balance between those rights and employers' legitimate business-related interests. Federal legislation is the best solution to clean up the wide disparity among the state statutes and bills. The Proposed Act set forth in this article is intended to help restore that balance. It defines the relevant terms, clearly describes the prohibited acts, and provides for reasonable exceptions for valid business-related purposes. Codification of this uniform standard would help to prevent the kinds of abuses described in the Introduction of this article while at the same time giving employers access to relevant information for legitimate business reasons.

Appendix A: Detailed Comparison of Password Privacy Legislation

State	*Applicable Parties*	*Online Accounts or Devices*	*Prohibited Acts*	*Exceptions/Exemptions*	*Enforcement Provisions and Penalties*	*Miscellaneous Provisions*
			ENACTED STATUTES			
Arkansas Ark. Code Ann. § 11-2-124 (West 2013)	• Private and public employers • Employees • Prospective employees	• Social media account • Names specific social networking sites	• Require, request, suggest, or cause • Prohibits employer from requiring employee or applicant to add employer to contact list • Prohibits employer from asking for changes to privacy settings • Prohibits retaliation • Inadvertently gaining access not prohibited	• Workplace misconduct investigations • Employer may search for information in the public domain	(No penalty or enforcement provision)	
California Cal. Lab. Code § 980 (West 2013)	• Private and public employers • Employees • Job applicants	• Social media	• Require or request • Prohibits shoulder surfing • Prohibits retaliation	• Workplace misconduct investigations	(No penalty or enforcement provision)	
Colorado Colo. Rev. Stat. Ann. § 8-2-127 (West 2013)	• Private and public employers • Employees • Job applicants	• Online personal account • Electronic communications device	• Require, request, suggest, or cause • Prohibits shoulder surfing • Prohibits employer from requiring employee or applicant to add employer to contact list • Prohibits employer from asking for changes to privacy settings • Prohibits retaliation	• Investigation into misappropriation of proprietary, confidential, or financial information • Employer may maintain workplace policies related to the Internet and electronic equipment	• Civil penalty of $1,000 • Injured party files complaint with state Labor & Employment Dept.	

Illinois 820 Ill. Comp. Stat. Ann. 55/10 (West 2012)	• Private and public employers • Employees • Prospective employees	• Social networking website	• Require or request • Prohibits shoulder surfing	• Employer may maintain workplace policies related to the Internet and electronic equipment • Employer may search for information in the public domain	(No penalty or enforcement provision)	
Louisiana 2014 La. Act 165 (to be codified at La. Rev. Stat. Ann. §§ 51:1951–1955 (2014)	• Private and public employers • Employees • Job applicants	• Personal online account • Electronic communications device	• Request or require • Prohibits retaliation	• May ask for access to employer's electronic communications device or account • Workplace misconduct investigations—but only allow employer to require employee to share necessary content • Investigation into misappropriation of proprietary, confidential, or financial information—but only allow employer to require employee to share necessary content • Employer may search for information in public domain	(No penalty or enforcement provision)	• Statute created new Personal Online Account Privacy Protection Act • Law does not prohibit employer from complying with a duty to screen employees or applicants • Law does not create duty to search or monitor online activity; employer will not be liable for failure to do so • Law does not prohibit or restrict an employee or applicant from "self-disclosing" username or password which allows access to employee's or applicant's personal online account
Maryland Md. Code Ann., Lab. & Empl. § 3-712 (West 2012)	• Private and public employers • Employees • Job applicants	• Personal account or service • Electronic communications device	• Request or require • Prohibits retaliation	• Investigation into misappropriation of proprietary, confidential, or financial information	(No penalty or enforcement provision)	

Appendix A: Continued

State	*Applicable Parties*	*Online Accounts or Devices*	*Prohibited Acts*	*Exceptions/Exemptions*	*Enforcement Provisions and Penalties*	*Miscellaneous Provisions*
Michigan Mich. Comp. Laws Ann. §§ 37.271–.278 (West 2012)	• Private and public employers • Employees • Job applicants	• Personal internet account	• Request • Prohibits shoulder surfing • Prohibits retaliation	• Workplace misconduct investigations • Investigation into misappropriation of proprietary, confidential, or financial information • Employer may search for information in the public domain	• Criminal penalty—misdemeanor ($1,000 fine) • Civil action—$1,000 in damages	• Statute created new Internet Privacy Protection Act • Law does not create a duty to search or monitor employee Internet use; employer will not be liable for failure to do so • Law not intended to hinder legal duty to conduct Internet searches on employees or applicants
Nevada Nev. Rev. Stat. Ann. § 613.135 (West 2013)	• Private and public employers • Employees • Prospective employees	• Social media account	• Require, request, suggest, or cause • Prohibits retaliation	• Workplace misconduct investigations	(No penalty or enforcement provision)	
New Jersey N.J. Stat. Ann. §§ 34:6B-5–10 (West 2013)	• Private and public employers • Employees • Job applicants	• Social networking website	• Require • Prohibits retaliation • Prohibits employers from inquiring about existence of social media account	(No exceptions or exemptions)	• Civil remedy—$1,000	• Prohibits employers from asking employee or applicant for a waiver of the provisions of the statute

New Mexico N.M. STAT. ANN. § 50-4-34 (West 2013)	• Employers (does not specify whether it applies to both private and public employer) • Job applicants	• Social networking website	• Require or request • Prohibits shoulder surfing	• Employer may maintain workplace policies related to the Internet and electronic equipment • Employer may search for information in the public domain • Federal, state or local law enforcement agencies exempt • Employer may ask for password information to access its own internal systems or equipment	(No penalty or enforcement provision)	
Oklahoma H.B. 2372, Reg. Sess. (Okla. 2014) (to be codified at OKLA. STAT. ANN. tit. 40, §§ 173.2, 173.3 (West 2014)) (effective Nov. 1, 2014)	• Employers (does not specify whether it applies to both private and public employer) • Employees • Prospective employees	• Personal online social media account	• Require • Prohibits shoulder surfing • Prohibits retaliation	• Employer may ask for password information to access employers devices or accounts • Workplace misconduct investigations • Investigation into unauthorized transfer of proprietary, confidential, or financial information	Civil remedy —$500	• Punitive or emotional damages are not recoverable • Statute may not be used "for the basis of a public policy tort." • Employer not liable for failure to review employee's personal online social media account • Employer's failure to access this information is not admissible in any legal proceeding
Oregon OR. REV. STAT. § 659A.330 (West 2014)	• Private and public employers • Employees • Job applicants	• Social media	• Require or request • Prohibits shoulder surfing • Prohibits employer from requiring employee or applicant to add employer to contact list • Prohibits retaliation	• May ask for password information to access employer's account • Workplace misconduct investigations—but only allow employer to require employee to share necessary content • Employer may search for information in the public domain	(No penalty or enforcement provision)	• Law does not create a duty to search or monitor employee Internet use; employer will not be liable for failure to do so

Appendix A: Continued

State	*Applicable Parties*	*Online Accounts or Devices*	*Prohibited Acts*	*Exceptions/Exemptions*	*Enforcement Provisions and Penalties*	*Miscellaneous Provisions*
Rhode Island 2014 R.I. Pub. Law S2095A (to be codified at R.I. Gen. Laws Ann. § 28-56-1–6 (West 2014) (effective June 30, 2014).	• Private and public employers • Employees • Job applicants	• Social media account	• Require, coerce or request • Prohibits shoulder surfing • Prohibits employer from requiring employee or applicant to add employer to contact list • Prohibits employer from asking for changes to privacy settings • Prohibits retaliation	• Workplace misconduct investigations • Employer may search for information in the public domain	• Civil remedy —(no dollar amount specified)	• Law shall not restrict legal duty to screen employees or applicants, or to retain employee communications as required by federal law related to financial institutions or securities regulation
Tennessee Tenn. Pub. Act No. 2014-826 (effective Jan. 1, 2015)	• Private and public employers • Employees • Job applicants	• Personal internet account	• Request or require • Prohibits shoulder surfing • Prohibits employer from requiring employee or applicant to add employer to contact list • Prohibits retaliation	• May ask for access information to access employer's electronic communications device or account • Investigation into misappropriation of proprietary, confidential, or financial information —but only allow employer to require employee to share necessary content • Workplace misconduct investigations • Employer may search for information in the public domain	• Civil remedy—$1,000 • Attorney general may bring a civil action against employer on behalf of employee or applicant • Individual employee or applicant may also bring a civil action	• Statute created new Employee Online Privacy Act of 2014

Utah Utah Code Ann. §§ 34-48-101–301 (West 2013)	• Private and public employers • Employees • Job applicants	• Personal internet account • Nonpersonal account implied	• Request • Prohibits retaliation	• Workplace misconduct investigations	• Civil remedy —$500	• Statute created new Internet Employment Privacy Act • Law does not create a duty to search or monitor employee Internet use; employer will not be liable for failure to do so
Washington Wash. Rev. Code Ann. §§ 49.44.200, 205 (West 2013)	• Private and public employers • Employees • Job applicants	• Social networking account	• Require, request, suggest, cause, or otherwise coerce. • Prohibits shoulder surfing • Prohibits employer from requiring employee or applicant to add employer to contact list • Prohibits employer from asking for changes to privacy settings • Prohibits retaliation	• Exempts platforms that facilitate work-related collaboration or exchanges of information	• Civil remedy—$500	
Wisconsin 2013 Wis. Act 208 (effective Apr. 10, 2014) (to be codified at Wis. Stat. Ann. § 995.55 (West 2014))	• Private and public employers • Employees • Applicants	• Personal internet account	• Request or require • Prohibits shoulder surfing • Prohibits retaliation	• May ask for access information to access employer's electronic communications device or account • Workplace misconduct investigations • Investigation into misappropriation of proprietary, confidential, or financial information—but only allow employer to require employee to share necessary content • May restrict employee's access to internet while using an employer-owned or provided electronic device • Employer may search for information in the public domain	• Civil penalty of $1,000 • Injured party files complaint with state department of workforce development	• Law not intended to hinder legal duty to screen applicants or monitor employee communications • Employer may request or require employee to disclose personal email address

Appendix A: Continued

State	*Applicable Parties*	*Online Accounts or Devices*	*Prohibited Acts*	*Exceptions/Exemptions*	*Enforcement Provisions and Penalties*	*Miscellaneous Provisions*
			SELECTED PROPOSED BILLS			
Connecticut S.B. 159, 2013 Gen. Assemb., Jan. Sess.	• Private and public employers • Employees • Applicants	• Personal online account	• Request or require • Prohibits retaliation	(No exceptions or exemptions)	• Civil penalty of not more than $10,000 • Allows for injunctive relief • Enforcement by Attorney General, who may bring an action in Superior Court	
Maine L.B. 1194, 2013 Leg., 1st Reg. Sess. (Me. 2013)	• Private and public employers • Employees • Independent contractors	• Personal e-mail account • Social media account	• Require or cause disclosure • Prohibits compelling an employee to add employer to contact list • Prohibits retaliation	• Act does not apply to information that is publicly available	• Treble damages • Reinstatement • Civil damages of no more than $1,000 • Attorney General or affected employee or applicant may enforce	• Repeated attempts considered harassment and subject to additional civil penalties of $2,000
Nebraska L.B. 58, 103d Leg., 1st Sess. (Neb. 2013)	• Private and public employers • Employee • Job applicants	• Personal account	• Require or request login information • Also prohibits shoulder surfing and indirect access through the employee's or applicant's contact • Prohibits retaliation	• Employer may conduct investigations based upon receipt of information that employee wrongfully downloaded information • Employer may maintain relevant policies • Employer may request access to employer-owned devices or accounts • Employer may access information in the public domain	• Provides for a civil action (within one year) • Does not specify any dollar amount, but allows for actual damages	• Includes a waiver provision • Prohibits *employee* from downloading proprietary or financial data to a personal website or social networking site without authorization

New Hampshire H.B. 414, 2013 Leg., Reg. Sess. (N.H. 2013)	• Employer (does not specify whether it applies to both private and public employer) • Employee • Prospective employee	• Social media • Personal account	• Request or require • Prohibits access to login information, adding employer or agent to contact list, and changing privacy settings • Prohibits retaliation	• Allows employer to enforce relevant workplace policies • Employer may access information in the public domain • Employer may obtain information to ensure compliance with securities or financial laws	• Civil penalty imposed by labor commissioner	
North Dakota H.B. 1455, 63d Leg. Assemb. (N.D. 2013)	• Private or public employers • Employees • Applicants (only employers and applicants defined)	• Social networking site	• Require or request • Prohibits direct access, shoulder surfing, and indirect access through employee's or applicant's contacts • Prohibits retaliation	• Employer may enforce relevant workplace policies • Employer may request or require information for employer owned devices and accounts • Employer may access information in the public domain • Employer may conduct investigations about workplace misconduct and unauthorized downloading of proprietary or financial information	• Civil action (within one year) • Does not specify any dollar amount, but allows for actual damages	• Includes a waiver provision
Social Networking Online Protection Act (SNOPA) H.R. 537, 113th Cong. (1st Sess. 2013)	• Employer • Employee • Applicant for employment	• Private e-mail • Personal account . . . on any social networking website	• Unlawful to require or request • Prohibits retaliation	(No exceptions or exemptions)	• Civil penalty of not more than $10,000 • Allows for injunctive action • Enforcement by Secretary of Labor	