#PasswordProtection: Uncovering the Inefficiencies of, and Not-So-Urgent Need for, State Password-Protection Legislation

"Yes, there are many networks. Yes, they're thinning our attention. And, yes, this is the new form of media and influence, and it is transforming corporate communications, traditional media, and how people communicate with each other. The future of communications is already upon us. Get used to it."[1]

I. INTRODUCTION

"Buzzworthy," "BYOD" (bring your own device), and "selfie" have been added to the free Oxford Dictionaries Online after each word has worked its way into common usage or even into the respected print Oxford Dictionary.[2] "Friend" is no longer a mere noun or synonym for acquaintance, but instead, a verb to indicate adding an individual "to a list of friends or contacts on a social networking website."[3] For better or worse, social media impacts how individuals communicate and interact with one another, both online and in person and "[e]veryone is doing it."[4] In December 2014, a decade after its founding, Facebook had 1.39 billion monthly active users, 890 million daily active users, and over 1 billion active users of Facebook mobile products.[5]

1. Brian Solis, *Social Media Is About Sociology Not Technology*, BRIAN SOLIS (Aug. 28, 2007), http://www.briansolis.com/2007/08/social-media-is-about-sociology-not/, *archived at* http://perma.cc/66FZ3QC8.

2. *See* Valerie Strauss, *Twerk, MOOC, Girl Crush—Words Added to Oxford Dictionaries Online*, WASH. POST (Aug. 28, 2013), http://www.washingtonpost.com/blogs/answer-sheet/wp/2013/08/28/twerk-mooc-girl-crush-words-added-to-oxford-dictionaries-online/, *archived at* http://perma.cc/EYF8-FVSC (reporting words recently added to free online Oxford Dictionary).

3. *Friend*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/english/friend?q=friend (last visited Sept. 22, 2013), *archived at* http://perma.cc/N2KH-YTYL.

4. *See* Catherine Crane, Note, *Social Networking v. The Employment-at-Will Doctrine: A Potential Defense for Employees Fired for Facebooking, Terminated for Twittering, Booted for Blogging, and Sacked for Social Networking*, 89 WASH. U. L. REV. 639, 639 (2012) (detailing overwhelming popularity of Facebook). Due to Facebook and Twitter's ever-increasing popularity, Crane suggests that social media-related firings are unsurprising and predicts that the practice will accelerate as college-aged Facebook users enter the professional workforce. *See id.* at 639-40; *see also* Jeffrey A. Mello, *Social Media, Employee Privacy and Concerted Activity: Brave New World or Big Brother?*, 63 LABOR L.J. 165, 165 (2012) (describing changes brought by social media in professional and personal interaction). Social media has altered how individuals communicate in their personal interactions, and a majority of businesses use social networking as a professional tool for communications, recruiting, and marketing. *See* Mello, *supra*, at 165.

5. *See Newsroom*, FACEBOOK, http://newsroom.fb.com/company-info/ (last visited Mar. 26, 2015),

Other popular social media websites—Instagram, Twitter, and LinkedIn—indicate widespread and growing usage of the sites and social media overall.[6]

Given this relatively recent surge of sharing and interaction, social media use raises significant questions concerning what its users should consider private, particularly within the context of hiring and employment.[7] Different factors shape an employee's privacy expectations, such as: the privacy settings implemented by the account holder, the potential generational divide on what an individual considers public information, and the nature of the individual's employment.[8] While employee expectations of privacy are important, these expectations require a careful balance with the employer's needs for productivity and protection from liability for employee action on social media accounts.[9]

archived at http://perma.cc/D3U4-FVSJ (listing key facts and numbers concerning Facebook users worldwide).

6. *See* Bianca Bosker, *Twitter: We Now Have over 200 Million Accounts*, HUFFINGTON POST (Apr. 28, 2011), http://www.huffingtonpost.com/2011/04/28/twitter-number-of-users_n_855177.html, *archived at* http://perma.cc/EA6E-ZZ8X (stating Twitter revealed statistics of 200 million accounts); *300 Million Sharing Real Moments*, INSTAGRAM, blog.instagram.com/post/104847837897/141210-300million (last visited Mar. 26, 2015), *archived at* http://perma.cc/ZE55-8UBE (providing statistics of 300 million active users); *About LinkedIn*, LINKEDIN, http://press.linkedin.com/about (last visited Mar. 26, 2014), *archived at* http://perma.cc/D28X-H6AT (declaring over 332 million users for professional networking site).

7. *See* Patricia Sanchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 64 (2012) ("[T]raditional professionalism demands audience segregation between the employee's professional and private personas."). In spite of the professionalism typically demanded in the workplace, "millennials" appear unwilling to sacrifice their Internet presence for employers and "rely on others, including employers, to refrain from judging them across contexts." *Id.* at 66.

8. *See* Alissa Del Riego et al., *Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy*, 16 J. INTERNET L., no. 3, 2012, at 1, 19 (asserting password-protected accounts suggest privacy expectation exists, but "calibration of privacy . . . settings" also important). The degree to which a user protects his or her "digital information" helps determine whether a privacy expectation reasonably exists. *See id.*; Steven D. Zansberg & Janna K. Fischer, *Privacy Expectations in Online Social Media—An Emerging Generational Divide?*, 28-NOV COMM. LAW. 1, 29 (2011) (comparing Internet use of older "digital immigrants" with younger "digital natives"). Those who grew up with Facebook ("digital natives") tend to treat the Internet as public, whereas "digital immigrants" who lived and matured prior to Facebook and social media are more likely to believe that their posts are private and that they choose who can see their information. *See* Zansberg & Fischer, *supra*, at 29; Crane, *supra* note 4, at 644 (stating Constitution affords greater free speech protection to public employees than private employees); *see also* Francois Quintin Cilliers, *The Role and Effect of Social Media in the Workplace*, 40 N. KY. L. REV. 567, 568 (2013) (citing majority of surveyed college students would refuse job banning social media, or circumvent policy).

9. *See* Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 STAN. TECH. L. REV. 7, 26 (2012) (noting employer must mitigate risks of employee social media use). Such risks include "trade secret disclosures, losses of productivity, violations of anti-spam laws, harassment of co-workers, third party copyright infringements, [and] illegal endorsements." *Id.*; *see also* Leslie Hayes & Sally J. Cooley, *Social Media—Striking the Balance Between Employer and Employee*, 55 IDAHO ST. B. ADVOC. 22, 24 (2012), *available at* http://isb.idaho.gov/pdf/advocate/issues/adv12novdec.pdf, *archived at* http://perma.cc/6MVR-ZY9J (recommending employers create clear and specified social media policy for protection). "A good policy will put an employee on notice of the expectation, but still permit protected activity." Hayes & Cooley, *supra*, at 167; *see also* Mello, *supra* note 4, at 3 ("[E]mployer monitoring of employee communications is not only legal but also practical, given the nature and reach of electronic communications."); Michelle Sherman, *Social Media and Employers: Finding the Right Balance Between Two Extremes—Asking for Facebook Passwords and Thinking You Can Ignore Social Media*, 17 CYBERSPACE LAW., no. 5, 2012, at 14 (reviewing potential

The rise of modern technology in the personal and professional spheres leaves courts and legislatures in "sticky" situations to determine employee online privacy rights.[10] More recently, over thirty-five state legislatures have proposed or adopted legislation to protect employees, applicants, and, in some states, students in higher education from employer or institutional administrative requests for social media usernames and passwords.[11] As of late 2013, fourteen states have enacted password-protection legislation.[12] The recent demand for such protection ultimately stems from the Maryland Department of Corrections' demand to access the social media passwords of an applicant, Robert Collins, to ensure that he was not affiliated with any gangs.[13] The practice, which Facebook's Terms of Service prohibit, prompted an outcry from the American Civil Liberties Union (ACLU) and gained the attention of

employee concerns over trade secrets, discrimination claims, and negligent hiring); *cf.* Stephanie Clifford, *Video Prank at Domino's Taints Brand*, N.Y. TIMES (Apr. 15, 2009), http://www.nytimes.com/2009/04/16/business/media/16dominos.html?_r=0 (reporting employee fired for posting prank video of tampering with food, consequently damaging Domino's reputation).

10. *See* Del Riego et al., *supra* note 8, at 18 (claiming current law incomplete, obsolete, or stretched). Although courts do address the issue, their fact-specific rulings do not offer guidance to employers and employees. *See id.*

11. *See Employer Access to Social Media Usernames and Passwords Legislation: 2013*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx#2013 (last visited Mar. 26, 2015), *archived at* http://perma.cc/5FWJ-574D [hereinafter *2013 State Bills and Laws*] (detailing current pending and passed state password-protection legislation); *see also* Freeland Cooper, *Employees, Politicians Balk at Employers Seeking Social Media Passwords*, 22 CAL. EMP. L. LETTER, no. 2, 2013, at 11 (noting several states "mulling" password-protection legislation and U.S. senators requested investigations); Alan Gutterman, *States Begin Push for Implementation of Employee Password Protection Laws*, LEGAL SOLUTIONS BLOG (Oct. 12, 2012), http://blog.legalsolutions.thomsonreuters.com/law-and-techology/states-begin-push-for-implementation-of-employee-password-protection-laws/, *archived at* http://perma.cc/46WH-NRJP ("California is actually just one of several states that has been considering, and implementing 'password protection' laws . . . .").

12. *See 2013 State Bills and Laws*, *supra* note 11 (indicating state bills enacted as of September 2013). These states include Arkansas, Colorado, Nevada, New Mexico, Oregon, Utah, Vermont, and Washington in 2013, and California, Delaware, Illinois, Maryland, Michigan, and New Jersey in 2012. *Id.*; *see also Employer Access to Social Media Usernames and Passwords: 2012 Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 17, 2013), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx, *archived at* https://perma.cc/VB3E-X7R2. As of November 2014, Louisiana, Maine, New Hampshire, Oklahoma, Rhode Island, Tennessee, and Wisconsin have enacted password-protection legislation beyond the focus of this paper. *See Employer Access to Social Media Usernames and Passwords: Legislation 2014*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014 (last visited Mar. 26, 2015), *archived at* https://perma.cc/U6KD-FGEM (noting seven states adopting legislation and at least twenty-eight with pending legislation in November 2014).

13. *See* Michelle Scheinman, *Cyberfrontier: New Guidelines for Employers Regarding Employee Social Media*, 44 MCGEORGE L. REV. 731, 731 (2013) (describing why Collins felt compelled to disclose his Facebook password to Maryland Department of Corrections). After taking a brief leave of absence, Collins feared that he would not be reinstated in his position with the department if he failed to capitulate to his employer's demands. *See id.*; Katy Steinmetz, *States Rush To Ban Employers from Asking for Social Media Passwords*, TIME (Apr. 9, 2013), http://swampland.time.com/2013/04/09/states-rush-to-ban-employers-from-asking-for-social-media-passwords/, *archived at* http://perma.cc/9GUN-8VYT (explaining employer demand to access Collins's Facebook account, including his personal messages and photos).

federal lawmakers.[14] Despite the backlash, however, this practice is not widespread or commonplace.[15]

This Note will first explore the sources of employee privacy protection in the digital age prior to the call for password-protection legislation.[16] Although many of these protections—including the Stored Communications Act (SCA) and the National Labor Relations Act (NLRA)—are arguably obsolete, courts have interpreted the language of such acts to apply to the current technological landscape, including social media.[17] This Note will then analyze and compare

14. *See* Ategah Khaki, *Status Update: Employers Asking for Your Facebook Password Violates Your Privacy and the Privacy of All Your Friends, Too*, ACLU (Mar. 22, 2012), https://www.aclu.org/blog/technology-and-liberty/status-update-employers-asking-your-facebook-password-violates-your, *archived at* http://perma.cc/VF6A-KGKF (responding to incident involving Collins and Maryland DOC); Press Release, Senators Richard Blumenthal & Chuck Shumer, Employer Demands for Facebook and Email Passwords as Precondition for Job Interviews May Be a Violation of Federal Law; Senators Ask Feds To Investigate (Mar. 25, 2012), http://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-schumer-employer-demands-forfacebook-and-email-passwords-as-precondition-for-job-interviews-may-be-a-violation-of-federal-law-senators-askfeds-to-investigate, *archived at* http://perma.cc/YYG8-KZYR (detailing senators' request for investigation into employers asking for social media passwords); *Statements of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last visited Feb. 2, 2015), *archived at* http://perma.cc/AZV2-NHNC ("You will not share your password . . . let anyone else access your account, or do anything else that might jeopardize the security of your account.").

15. *See* Cooper, *supra* note 11 ("[L]ater news reports indicated that few employers actually request passwords, [but] there's been a big backlash."); Del Riego et al., *supra* note 8, at 18 (stating password request practice not commonplace, but gaining attention); Steinmetz, *supra* note 13, (reporting ACLU as "predictably appalled" by practice). Despite a "dearth of data about how many employers . . . out there are actually demanding access," legislatures have quickly responded to the practice. Steinmetz, *supra* note 13.

16. *See* Kelly Schoening & Kelli Kleisinger, *Off-Duty Privacy: How Far Can Employers Go?*, 37 N. KY. L. REV. 287, 312-18 (2010) (outlining NLRB and SCA protections for employees); 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, 495-500 (2011) (reviewing purpose and background of SCA); *see also infra* Part II.A.

17. *See* Stored Communications Act, § 201, 18 U.S.C. §§ 2701-2711 (2012) (protecting stored communications accessed without authorization); National Labor Relations Act, §§ 1-19, 29 U.S.C. §§ 151-169 (2012) (prohibiting unfair labor practices); *see also* 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, 77-78 (2011) (reviewing SCA and asserting its obsolescence within current technological landscape). Baker argues that the SCA is not suited for modern communications and legislators should "either radically reform or completely replace the SCA." Baker, *supra*, at 78; Memorandum OM 11-74 from Anne Purcell, Assoc. Gen. Counsel, Nat'l Labor Relations Bd., to All Reg'l Dirs., Officers-in-Charge, and Resident Officers (Aug. 18, 2011) [hereinafter August 2011 Memo], *available at* http://www.nlrb.gov/reports-guidance/operations-management-memos (click "Memo Number" drop-down menu; then select "OM 11-XX"; then click "Apply"; then click link for "OM 11-74" to open or download) (reporting recent case developments in social media); Memorandum OM 12-31 from Anne Purcell, Assoc. Gen. Counsel, Nat'l Labor Relations Bd., to All Reg'l Dirs., Officers-in-Charge, and Resident Officers (Jan. 24, 2012) [hereinafter January 2012 Memo], *available at* http://www.nlrb.gov/reports-guidance/operations-management-memos (click "Memo Number" drop-down menu; then select "OM 12-XX"; then click "Apply"; then click "3" at bottom of page; then click link for "OM 12-31" to open or download) (issuing second report to thoroughly consider social media cases); Memorandum OM 12-59 from Anne Purcell, Assoc. Gen. Counsel, Nat'l Labor Relations Bd., to All Reg'l Dirs., Officers-in-Charge, and Resident Officers (May 30, 2012) [hereinafter May 2012 Memo], *available at* http://www.nlrb.gov/reports-guidance/operations-management-memos (click "Memo Number" drop-down menu; then select "OM 12-XX"; then click "Apply";

current password-protection legislation, as well as pending legislation at the federal level—the Social Networking Online Protection Act (SNOPA), and the Password Protection Act (PPA).[18] Part III of this Note asserts that current statutory provisions may already sufficiently protect employees and argues that proposed legislation should avoid ambiguity and strive to create exceptions that strike an appropriate balance between employer needs and employee privacy.[19] Finally, this Note proposes that employee self-regulation and clearly defined employer social media policies are the most effective and proactive methods of navigating the vague and varied legislation that attempts to police password-requesting practices.[20]

II. HISTORY

A. Potential Causes of Action Related to Social Media

Although there is a current push for password-protection laws at both the state and federal levels, several statutory and common law rights already exist that might offer similar protection to employees.[21] This Note will explore these protections and their applications to social media in the context of employment in the following sections.[22]

then click "2" at bottom of page; then click link for "OM 12-59" to open or download) (issuing final report covering social media issues).

18. *See infra* Part II.C.2 (discussing pending legislation); *see also* Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013) (attempting to restrict employer requests for employee social media passwords); Password Protection Act of 2013, S. 1426, 113th Cong. (2013) (prohibiting employer access to or demands for employee information on protected computer).

19. *See* Mark Bannister et al., *Employer Use of Facebook and Other Social Media in Hiring*, J. KAN. B. ASS'N, June 2013, at 20, 30 (noting valid reasons employers reject applicants based on information on social media sites); Robert Sprague, *Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship*, 50 U. LOUISVILLE L. REV. 1, 31-34 (2011) (summarizing best practices for employer and employee concerning social media). Employers must remain vigilant of both the law and employee activity as social networking becomes more prominent in the professional world. *See* Sprague, *supra*, at 31-34 (reminding employer to be mindful of "legal minefields" surrounding social networking issues with employers); *see also* Kara E. Shea, *The Buzz About Social Media Password Laws*, 27 TENN. EMP. L. LETTER, no. 7, 2012, at 3 (suggesting password legislation fails to protect employers in necessary workplace investigations and against negligent hiring); 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, 884-91 (2013) (proposing federal legislation will improve existing laws and should borrow from successful state measures).

20. *See infra* Part III.D; *see also* Kevin W. Mahoney, *Social Media Policies: Enter at Your Own Risk*, 272 N.J. LAW. 27, 31 (2011) (asserting importance of comprehensive social media policy by employer); Bethany N. Whitfield, Comment, *Social Media @ Work: #PolicyNeeded*, 66 ARK. L. REV. 843, 875-76 (2013) (encouraging employer to actively manage social media and use specific policies).

21. *See infra* Part II.A.1-4 (demonstrating protections offered by Constitution, SCA, NLRA, and various other actions).

22. *See infra* Part II.A.1-4.

1. Constitutional Claims

Although this Note primarily focuses on password-protection of private employees, First Amendment and Fourth Amendment protections do protect public employees, in ways that may extend to social media rights and protections.[23] If statements made on a social networking website pertain to a matter of public concern, such comments fall under the First Amendment's protection and require courts to balance the employee's interest (as a citizen commenting on a matter of public concern) against the employer's interest in "promoting the efficiency of the public services it performs through its employees."[24] A public employee's First Amendment protections may or may not extend to social media statements or comments, depending on the degree to which such statements disrupt the public service.[25]

While Fourth Amendment privacy protection extends to public employees, an important exception exists where an employer legitimately needs to monitor employees in order to ensure a successful working environment.[26] The landmark Supreme Court case *O'Connor v. Ortega*[27] determined that an individual's right to privacy in the workplace required a balance between the employee's legitimate expectation of privacy and the government's need to ensure effective and efficient operation of its agencies.[28] The Court declined to apply an "unrealistic" probable cause standard to non-law enforcement employees for such searches and instead applied a reasonableness standard to help ensure both public employee privacy as well as employer interest in competently conducting proper business.[29]

23. *See* U.S. CONST. amend. I (protecting freedom of press); U.S. CONST. amend. IV (preventing illegal searches and seizures); *see also* Franklin G. Shuler Jr. & Michelle Clayton, *When Is Private Not Really Private?: Privacy Interest in Employment After* Quon, 53 DRI FOR DEF., no. 6, 2011, at 61, 61 (stating public employers subject to restraints of constitutional amendments).

24. Pickering v. Bd. of Educ., 391 U.S. 563, 568 (1968); *see* Curran v. Cousins, 509 F.3d 36, 44-45 (1st Cir. 2007) (describing application of balancing test). In *Curran*, a disciplinary hearing resulted in the plaintiff's termination after he posted inappropriate comments to a union website while he was on suspension. *See* 509 F.3d at 42-43.

25. *See Curran*, 509 F.3d at 48-49 (holding posting "urged Department administrators to engage in insubordination" and justified plaintiff's termination). In *Curran* the court relied on the test the Supreme Court laid out in *Garcetti v. Ceballos*, which states that "[a] government entity has broader discretion to restrict speech when it acts in its role as employer, but the restrictions it imposes must be directed at speech that has some potential to affect the entity's operations." *Id.* at 45 (quoting Garcetti v. Ceballos, 547 U.S. 410, 418 (2006)). The *Garcetti* Court distilled this formulation from *Pickering*. *See Garcetti*, 547 U.S. at 418.

26. *See* Alexander Naito, Comment, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. PA. J. CONST. L. 849, 856-57 (2012) (exploring background on Fourth Amendment rights of public employees). Although the Fourth Amendment privacy protections extend to public employees, "that protection is limited by the legitimate needs of public employers to monitor employees and ensure a safe and efficient working environment." *Id.* at 857.

27. 480 U.S. 709 (1987) (plurality opinion).

28. *See id.* at 724. The Court here deemed the search of a medical professional's office valid on the basis that the intrusion was reasonable as it was in pursuit of government property. *See id.* at 728.

29. *See id.* at 724-25 (holding probable cause standard impractical for "legitimate work-related,

More recently, the Supreme Court grappled with the *O'Connor* framework in *City of Ontario v. Quon*,[30] specifically as it applies to modern cellular phones and text messages.[31] In *Quon*, the Court ultimately held that an employer's audit of a public employee's text messages was constitutional because the employer's policy suggested it was unreasonable for the employee to expect his excessive and nonwork-related text messages—even ones containing private information—were "free from scrutiny."[32] Although Fourth Amendment protection might not extend to social media under this analysis, these constitutional implications place important limits on a public employer, and courts have adopted the framework elsewhere to consider emerging technologies.[33]

2. The Stored Communications Act

The SCA is a component of the Electronic Communications Privacy Act of 1986 (ECPA) and governs online privacy protection and disclosure.[34] The statute protects against unauthorized access to stored communications.[35]

noninvestigatory intrusions [and] investigations of work-related misconduct"); *see also* Michael Z. Green, *Against Employer Dumpster-Diving for Email*, 64 S.C. L. REV. 323, 337 (2012) (discussing Fourth Amendment balancing test in workplace). In a two-part test, the *O'Connor* Court first considered the actual workplace to determine whether the employee had a legitimate expectation of privacy, and second, whether the employer intrusions were reasonable under the circumstances. *See* Green, *supra*, at 337. *But see O'Connor*, 480 U.S. at 729-32 (Scalia, J., concurring) (rejecting plurality and concluding government employee offices generally covered by Fourth Amendment). Justice Scalia noted, however, that "government searches to retrieve work-related materials or to investigate violations . . . are regarded as reasonable and normal in the private-employer context [and] do not violate the Fourth Amendment." *Id*. at 732.

30. 560 U.S. 746 (2010).

31. *See id.* at 746 (considering Fourth Amendment protection of police sergeant's text messages).

32. *Id.* at 762 (holding circumstances of employment suggested employee had no reasonable expectation of privacy). The Court upheld the search's constitutionality as being predicated on a legitimate, work-related purpose, within a limited scope, and reasonable under both the *O'Connor* plurality and concurrence. *See id.* at 764-65.

33. *See* Naito, *supra* note 26, at 867-68 (suggesting *Quon* framework will not generally provide expectation of privacy to social media). Naito argues, however, that social media *could* be incorporated into Fourth Amendment analyses if courts do not dismiss social media based on its "sharing component," but instead "analyze on a case-by-case basis whether an expectation of privacy exists . . . ." *Id.* at 877. Furthermore, Naito asserts that the scope of protection should depend on the workplace's relationship to social media and online activity. *See id.* at 878 ("[S]cope of protection would depend on the nature of the workplace."). There should be no expectation of privacy where the social media activity ostensibly relates to the employee's work. *See id.* The expectation should persist, however, where the employment has no relationship to social media. *See id.* at 878; *see also supra* notes 23-32 and accompanying text (discussing relevant cases and articles concerning public employee constitutional rights). On the public-employee level, these constitutional concerns and related cases provide an analytical framework for an employee's reasonable expectations in the workplace. *See supra* notes 23-32 and accompanying text.

34. *See* Feuer, *supra* note 16, at 496-99 (reviewing purpose of SCA).

35. 18 U.S.C. § 2701(a) (2012) (setting forth elements of violation). The SCA provides that whoever "intentionally accesses without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access . . . while it is in electronic storage . . . shall be punished."

Congress designed the SCA to protect modern concepts of privacy that emerged with technological development by protecting the privacy of complex electronic communication services (ECS) and remote computing services (RCS).[36] Congress enacted the SCA to enhance Fourth Amendment protections by restricting a provider from disclosing an individual's information and limiting the government's ability to require those disclosures.[37] Ultimately, Congress intended to protect private communications, not those available to the general public.[38]

Although courts have grappled with the SCA and its dated twentieth-century vision of technology, courts have applied the SCA's framework to present day social media legal issues.[39] As written, the SCA contains a "working definition" of storage, which requires a determination of whether electronic communications may be considered storage through ECS and RCS application.[40] Ultimately, the "authorization" required by the SCA must be divulged knowingly and voluntarily—not by demanding passwords or acquiring them through indirect means.[41] In order to establish a claim where access was unauthorized, it is important that the comment, posting, or statement be "private."[42]

a. Konop v. Hawaiian Airlines, Inc.

In *Konop v. Hawaiian Airlines, Inc.*,[43] the Ninth Circuit explored the SCA's application when an airline pilot filed a claim against his employer after the employer suspended the pilot for posting disparaging comments about his

36. *See* Feuer, *supra* note 16, at 497 (stating privacy protection afforded by SCA). ECS consists of any services that allow the users to send or receive wire or electronic communications. *See id.* at 497-98. ECS providers cannot knowingly divulge the contents of electronically stored communications to any person or entity without lawful consent. *See id.* at 498 (distinguishing RCS from ECS providers). RCS deals more with storage or processing services on an electronic communication system. *See id.*

37. *See* Baker, *supra* note 17, at 83-84 (explaining purpose of SCA).

38. *See* Feuer, *supra* note 16, at 498 (stating SCA protects private, not public communications).

39. *See id.* at 499 (describing Congress' failure to amend SCA resulted in "legal acrobatics" within court system).

40. *See* Nicholas Matlach, Comment, *Who Let the* Katz *Out? How the ECPA and SCA Fail To Apply to Modern Digital Communications and How Returning to the Principles in* Katz v. United States *Will Fix It*, 18 COMMLAW CONSPECTUS 421, 448-49 (2010) (describing court and legislative understanding of SCA "electronic storage" language).

41. *See* Nicholas D. Beadle, Note, *A Risk Not Worth the Reward: The Stored Communications Act and Employers' Collection of Employees' and Job Applicants' Social Networking Passwords*, 1 AM. U. BUS. L. REV. 397, 400 (2012) (defining SCA understanding of "authorization" within statute as applied by courts). Authorization is generally determined objectively, as courts question whether the authorizing party knew he or she granted the authorization, and whether the party voluntarily granted access to the otherwise hidden information. *See id.*

42. *See* Crane, *supra* note 4, at 663-64 (demonstrating SCA claims require accessed information not otherwise available to public).

43. 302 F.3d 868, 872-73 (9th Cir. 2002).

colleagues on his personal website.[44] Although the district court awarded summary judgment to the defendant, the Ninth Circuit reversed the ruling because the employee plaintiff posted on a secured website that the defendant employer only accessed after obtaining another employee's log-in information.[45] Based on the common sense application of the word "use" and "user" in the SCA, the court determined that the employer could not be considered a "user" of the website in question because his ability to merely view the information does not make him a "user."[46]

b. Pietrylo v. Hillstone Restaurant Group

In 2009, the Federal District Court for the District of New Jersey applied the SCA to postings on a private, invitation-only group on MySpace.com (arguably Facebook's predecessor in social networking) in *Pietrylo v. Hillstone Restaurant Group*.[47] The court considered the plaintiff employee's SCA claim where a manager compelled the plaintiff's coworker to disclose her log-in information so that the employer could access the group webpage.[48] The coworker felt coerced to provide her "authorization," as she feared the defendant employer would otherwise retaliate against her.[49] As such, the court denied the employer defendant's motion for judgment as a matter of law (JMOL) and motion for a new trial, holding that a reasonable jury could infer that the managers knew that they lacked proper authorization to view the websites at issue and accessed it multiple times when the employee unmistakably intended that the website remain private.[50]

c. Crispin v. Christian Audigier, Inc.

Crispin v. Christian Audigier, Inc.[51] demonstrates how courts struggle to apply the language of the SCA to present day social media legal issues.[52] In

44. *See id.* (reviewing facts of lawsuit).

45. *See id.* at 879-80 (describing Ninth Circuit's reasoning in reversing district court grant of summary judgment).

46. *See id.* at 880 (reversing summary judgment because defendant not considered "user" of secure website within SCA definition); *see also* Schoening & Kleisinger, *supra* note 16, at 315 (stating recent cases found SCA "more beneficial to employees than originally thought"). Schoening and Kleisinger propose that the court in *Konop* upheld the SCA protections through a technical loophole, but nevertheless ruled in favor of the employee. *See* Schoening & Kleisinger, *supra* note 16, at 315.

47. No. 06-5754(FSH), 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009) (stating MySpace group posting as cause for dispute); *see also* Scheinman, *supra* note 13, at 737 (noting few cases currently deal with right of employer access to employee social media).

48. *See Pietrylo*, 2009 WL 3128420, at *1, *3 (reviewing plaintiff argument revealing employer accessed MySpace page without authorization).

49. *See id.* at *3 (holding coworker's purported authorization as "coerced or provided under pressure").

50. *See id.* (stating rationale for rejecting defendant's motions for new trial and JMOL).

51. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

52. *See* Baker, *supra*, note 17, at 91 (stating no court directly addressed SCA application to social media sites until *Crispin*).

Crispin, the plaintiff—after filing a breach of contract claim against the defendant for sublicensing his artwork without consent—attempted to quash the defendant's subpoenas served on his Media Temple, Facebook, and MySpace sites on the grounds that the SCA protected such information.[53] The *Crispin* court ultimately determined that messages on social media websites may be considered akin to email or messages intended to reach a private bulletin board service (BBS), and thus, these messages qualified for protection under the SCA as an ECS provider.[54] Facebook "wall" postings or comments, however, presented a difficult and distinct question that the *Crispin* court could not resolve without knowing whether or not such information was publicly available or whether access was limited to a few individuals, and thus the court remanded in order to evaluate this question.[55]

3. The National Labor Relations Act

Under Section 7 of the NLRA, employees have the right to "self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage *in other concerted activities* for the purpose of collective bargaining."[56] Moreover, in Section 8(a)(1), the Act prohibits, as an unfair labor practice, employer interference with, restraint, or coercion of employees' rights guaranteed in Section 7.[57] The National Relations Labor Board (NLRB) expressed that "concerted activity" within the NLRA includes both outright and implicit surveillance of employees and specifically encourages employee union activity.[58] The NLRB extended surveillance protections to social media use because employees could potentially use social networking and media in order to perform these concerted activities.[59]

53. *See Crispin*, 717 F. Supp. 2d at 968-69 (detailing facts comprising complaint).

54. *See id.* at 980-81 (determining messaging services on social media sites qualify as ECS). The SCA should protect email, private BBS, and messaging taking place on social media websites as long as it remains private because legislative history suggests that Congress wanted to protect private electronic communications. *See id.* at 981 (expanding court's reasoning).

55. *See id.* at 991 (holding remand needed to determine wall posting status); *see also* Darin M. Klemchuk & Sita Desai, *Can Employer Monitoring of Employee Social Media Violate the Electronic Communications Privacy Act?*, 26 INTELL. PROP & TECH. L.J., no. 2, 2014, at 9, 11 (noting SCA protection depends, in part, on public availability of post or information).

56. 29 U.S.C. § 157 (2012) (emphasis added); *see* Sarah D. Davis, Student Comment, *Social Media Activity & The Workplace: Updating the Status of Social Media*, 39 OHIO N.U. L. REV. 359, 365 (2012) (stating social media issue largely focuses on what constitutes "protected concerted activity").

57. *See* 29 U.S.C. § 158(a)(1) (2012) (prohibiting employer action having any chilling effect on § 157 employee rights).

58. *See* James R. Glenn, Recent Development, *Can Friendly Go Too Far? Ramifications of the NLRA on Employer Practices in a Digital World*, 2012 U. ILL. J.L. TECH. & POL'Y 219, 224-25 (2012) (explaining NLRA protections from surveillance).

59. *See id.* at 225 (stating NLRB protection extended to prevent discrimination and in support of unionization).

In response to the increased impact of social media within the employment context, the NLRB released three memoranda between 2011 and 2012 that outlined social media cases occurring during that time frame and suggested appropriate workplace social media policies under Section 7.[60] The Board issued these reports to "ensure consistent enforcement actions, and in response to requests from employers for guidance in this developing area."[61] In the first report, the Office of General Counsel found that employees had engaged in "protected concerted activities" when discussing the terms and conditions of their employment with colleagues.[62] In another instance, the Board did not consider an employee's postings on Twitter concerted activity because the tweets posted on a work-related account were unprofessional, inappropriate, and did not relate to terms of employment or employee discussions.[63] In the fall of 2012, the Board began to establish precedent in social media cases by issuing decisions that involved discipline for social media postings.[64]

The NLRB also warned employers to ensure that their social media policies are not overly broad or vague.[65] The Board explained through memoranda and case law that an employer violates the NLRA if its policy "chills" employees in their exercise of Section 7 rights.[66] Furthermore, ambiguous rules that "contain

60. *See generally* August 2011 Memo, *supra* note 17; January 2012 Memo, s*upra* note 17; May 2012 Memo, *supra* note 17 (reporting recent case developments arising in social media context).

61. *The NLRB and Social Media*, NAT'L LABOR RELATIONS BD., *available at* http://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media (last visited Mar. 30, 2015), *archived at* http://perma.cc/CB8H-BBS2 (stating reasons for releasing memoranda on social media policy). After investigating various disciplinary actions against employees for their social media use, the Board found "reasonable cause to believe that some policies and disciplinary actions violated federal labor law." *Id.*

62. *See* August 2011 Memo, *supra* note 17, at *2 (characterizing employee Facebook postings concerning job performance as protected concerted activity). Even though the employee conversation occurred through social media, the conversation concerned working conditions and the posting employee intended to initiate a discussion amongst coworkers and sought their assistance. *Id.* at *3. The NLRA protected this employee's statements because the statements were not disparaging and for the above-stated reasons. *See id.*

63. *See id.* at *11 (stating employee discharge appropriate in response to unprofessional tweets). In this instance, the Board did not consider the activity protected because the tweets had no relation to the employee's job and did not seek to involve other employees in employment-related issues. *See id.* at *12.

64. *See The NLRB and Social Media*, *supra* note 61 (describing precedential value of social media cases before NLRB); *see also* Hispanics United of Buffalo, Inc., 359 N.L.R.B. No. 37 (Dec. 14, 2012) (holding discussion among coworkers fell within Act's protection). In this case, the Board held that the employee's intention in complaining to her coworkers "had the clear 'mutual aid' objective of preparing her coworkers for a group defense to those complaints." *Id.* at *3.

65. *See* May 2012 Memo, *supra* note 17, at *3 (defining overbroad social media policies and suggesting methods aiding in conforming to NLRB standards); *Chapter 12: National Labor Relations Act § 12-3(b)(2)*, *in* LABOR AND EMPLOYMENT IN MASSACHUSETTS: A GUIDE TO EMPLOYMENT LAWS, REGULATIONS & PRACTICES (2014) (advising Massachusetts employers on successful social media policies). This Massachusetts social media policy guide suggests that employees: know and follow the rules, be respectful, be honest and accurate, post only appropriate and respectful content, refrain from using social media where unrelated to work, and establish that retaliation from employers is prohibited. *See Chapter 12: National Labor Relations Act § 12-3(b)(2)*, *supra.*

66. *See* May 2012 Memo, *supra* note 17, at 2 (explaining pitfalls of overbroad policies). Even where a rule does not explicitly restrict protected activities, the employer might still violate the NLRA if employees

no limiting language or context that would clarify to employees that the rule does not restrict Section 7 rights are unlawful."[67] For example, an employer may not require "courtesy" from employees because even "disrespectful" conduct or language can encompass Section 7 activity "such as employees' protected statements . . . that object to their working conditions and seek the support of others in improving them."[68] Clearly stated rules that define their restrictions and scope to exclude protected activity, however, are not unlawful.[69] In its decisions, the NLRB ultimately integrated social media communications within the NLRA, treating online conversations similarly to more traditional "water cooler" conversation.[70]

4. Other Potential Actions

Although an employee might reasonably bring one of the following claims against an employer, courts have not necessarily explored each potential action's application to social media. In the case of privacy torts, courts have largely found such claims unwarranted in the context of email and texting, and would likely produce a similar result for social media claims.[71]

a. Off-Duty Conduct Statutes

While the NLRB's holdings apply to work-related correspondence, many states also offer protection for an employee's off-duty conduct, including

would reasonably construe the language to prohibit Section 7 activity, the rule was promulgated in response to union activity, or the rule has been applied to restrict the exercise of Section 7 rights. *See id.*

67. *See id.* at 3 (prohibiting overbroad or ambiguous policies lacking context that might restrict employee Section 7 rights).

68. Karl Knauz Motors, Inc., 358 N.L.R.B. No. 164 (Sept. 28, 2012) (holding employer "courtesy" rule in violation of NLRA); *see also* Stephen W. Lyman, *NLRB Makes It Official—Requiring Employees To Be Courteous Is Unlawful*, HR INSIGHTS FOR HEALTH CARE (Oct. 24, 2012), http://blogs.hallrender.com/insights/2012/10/24/nlrb-makes-it-official-requiring-employees-to-be-courteous-is-unlawful/, *archived at* http://perma.cc/L6LK-UD3C (detailing *Karl Knauz Motors* decision). Lyman notes that even though the language broadly impinges on employee rights, employers still can discipline employees for social media posts in some circumstances, and that employers should practice caution when acting in response to employee social media posts. *See* Lyman, *supra.*

69. *See* May 2012 Memo, *supra* note 17, at 3 (explaining appropriate application and implementation of social media policies). *See generally* Sherman, *supra* note 9 (considering need to balance employer interest with employee rights and privacy in social media policy).

70. *See* Cilliers, *supra* note 8, at 574 (discussing NLRA application to social media postings); William A. Herbert, *Can't Escape from the Memory: Social Media and Public Sector Labor Law*, 40 N. KY. L. REV. 427, 442 (2013) (noting proliferation of social media cases under NLRA). In a series of decisions, the NLRB considered the legality of "adverse actions taken against employees for their posts and the lawfulness of employer social media policies." *Id. But see* Glenn, *supra* note 58, at 229 (suggesting shortcomings of NLRB memoranda). Potential gaps in protection may exist within the NLRA because it only protects employees participating in concerted activity related to surveillance. *See id.*

71. *See infra* Part II.A.4 (describing potential employee claims for discrimination, privacy, and off-duty conduct).

smoking and drinking.[72] Many state statutes specifically apply to employee tobacco use and prohibit employers from discriminating against smokers or users of other tobacco products, while others more broadly prohibit against discrimination based on use of "lawful products."[73] Other states have enacted even broader protections against "lifestyle discrimination."[74] Such protections may conceivably translate to social media postings or text messaging because courts might deem such actions as occurring off employers' premises during nonworking hours.[75]

b. Privacy

While the Fourth Amendment protects some privacy interests of public employees, common law rights might also protect an employee's privacy interest depending on his or her objective and subjective reasonable expectation of privacy.[76] Examples of these potential claims include: intrusion upon seclusion or solitude into plaintiff's private affairs; public disclosure of private facts; false light; and appropriation claims.[77] Although invasions into employee email might not amount to a highly offensive invasion, many American employees believe that such communication remains private, and previous cases suggest that a privacy claim relating to personal content available on the Internet might still be appropriate and actionable.[78]

72. *See* Cara Magatelli, Article, *Facebook Is Not Your Friend: Protecting a Private Employee's Expectation of Privacy in Social Networking Content in the Twenty-First Century Workplace*, 6 J. BUS. ENTREPRENEURSHIP & L. 103, 112-13 (2012) (explaining off-duty conduct statutes).

73. *See* Stephen Keyes, *Can Employees Be Fired for Off-Duty Smoking or Other Lawful Consumer Activities Outside of Work? (It Depends on What State They're In)*, 21 ANDREWS EMP. LITIG. REP., no. 24, 2007, at 2 (summarizing nineteen state statutes protecting tobacco use and other "lawful products"). Many statutes have specific exceptions, such as for state employees, where an organization exists to discourage use of tobacco products, or where the restriction relates to a bona fide occupational requirement. *See id.*

74. *See id.* (reviewing statutes broadly prohibiting discrimination against employees for otherwise lawful conduct); *see also* COLO. REV. STAT. § 24-34-402.5(1) (West 2015) ("It shall be a[n] . . . unfair employment practice . . . to terminate . . . any employee . . . engaging in any lawful activity off the premises of the employer during nonworking hours[.]"). This statute applies unless the restriction relates to a bona fide occupational requirement or is necessary to avoid a conflict of interest with the employer. *See* COLO. REV. STAT. § 24-34-402.5(1); *see also* CAL. LAB. CODE § 98.6 (West 2015) (protecting employees against employer retaliation for legal off-duty actions); N.Y. LAB. LAW § 201-d (McKinney 2015) (defining activities protected under New York labor law); N.D. CENT. CODE § 14-02.4-01 (2013) (protecting lawful off-duty conduct not directly conflicting with the employer's "business-related interests").

75. *See* Magatelli, *supra* note 72, at 112-19 (asserting off-duty conduct statutes apply to private activities). The scope of protection depends largely on the construction of the state's statute and its exceptions. *See id.* Thus, off-duty conduct statutes might protect employee conduct in one state, but in another that same activity might not be afforded similar protection. *See id.* (noting variation in statutory interpretation of off-duty conduct legislation).

76. *See* Diane Vaksdal Smith & Jacob Burg, *What Are the Limits of Employee Privacy?*, 29 GPSOLO, no. 6, 2012, at 8, 10 (considering employee right to privacy in public and private employment).

77. *See* Green, *supra* note 29, at 345 (listing tort actions in privacy claims).

78. *See id.* at 344-45 (suggesting privacy torts might not apply to employee email communication); *see also* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862 (Ct. App. 2009) (identifying MySpace

c. Discrimination Claims

Although courts have held that there is generally no reasonable expectation of privacy in one's workplace, a snooping employer still needs to be wary of what it uncovers on an employee's or applicant's social media webpage and consider the potential for discrimination claims.[79] The Civil Rights Act of 1964 prohibits employers from firing an employee or refusing to hire a candidate based on potentially discriminatory information.[80] The proliferation of social media has created potential situations where an employer not only learns relevant information about a candidate through a quick search, but at the same time may discover and expose protected information about a candidate that an employer may not legally consider in the hiring process.[81] Prehire social networking checks may create circumstantial evidence to support an inference that information available online about a candidate's protected group status unlawfully motivated an employment decision.[82]

B. The Demand for Increased Social Media Password Protection

In a 2010 interview with the Maryland Department of Corrections (DOC), Robert Collins's interviewer "demanded access to his Facebook account" and searched through his personal messages and photos in order to

comments as not private because of public availability). The court in *Moreno* determined that by submitting the plaintiff's statements to a local newspaper that were publicly available on her MySpace page at the time, the defendant's conduct did not create a cause of action for invasion of privacy. *See Moreno*, 91 Cal. Rptr. 3d at 862-63; *see also* McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, *1 (Tex. Ct. App. May 28, 1999) (detailing failed privacy tort action). In *McLaren v. Microsoft Corp.*, a Texas court determined that an employee's email on an employer-provided computer was not the employee's personal property. *See McLaren*, 1999 WL 339015, at *1. Moreover, the employee did not have a reasonable expectation of privacy because the statements traveled over the company's network, making them accessible to the employer. *See id.* at *4.

79. *See* Mello, *supra* note 4, at 3 (describing general lack of employee privacy in email); Sherman, *supra* note 9, at 1 (listing recent discrimination and other claims arising from hiring decisions based on social media information).

80. *See* 42 U.S.C. § 2000e-2(a)(1) (2012). "It shall be an unlawful employment practice for an employer . . . to fail or refuse to hire or to discharge any individual, or otherwise discriminate . . . because of such individual's race, color, religion, sex, or national origin." *Id.*

81. *See* Scott Brutocao, *Issue Spotting: The Multitude of Ways Social Media Impacts Employment Law and Litigation*, ADVOC. (TEX.), Fall 2012, at 8, 8 (explaining risks and potential benefit of employer searching employee's or applicant's social media presence).

82. *See* Megan Whitehill, Comment, *Better Safe than Subjective: The Problematic Intersection of Pre-Hire Social Networking Checks and Title VII Employment Discrimination*, 85 TEMP. L. REV. 229, 260 (2012) (asserting prehire social media checks creating implicit bias in employer). Whitehill explains, "proof that a prehire social networking profile evaluation occurred could be . . . offered to prove that protected group status was a motivating factor in the adverse employment decision." *Id.* at 261. In the instance where a candidate otherwise meets the employer's legitimate performance expectations, the candidate may then present sufficient evidence to create an inference of unlawful discrimination against an individual within a protected class—information of which an employer might only be aware of due to social media. *See id.* at 239 (explaining employee discrimination claims).

ensure that Collins was not affiliated with any gangs.[83] Stating that he had no choice but to provide the requested information or risk his recertification with the DOC, Collins obliged and subsequently brought his story to the ACLU, which issued a press release and provided Collins with a platform to air his grievances.[84] Collins's incident with a public employer and the ACLU's response elicited action in Maryland, making it the first state to pass a law prohibiting employers from demanding or requiring disclosure of an applicant's or employee's social media passwords.[85]

The ACLU's outrage against the practice quickly spread, and several state legislatures followed Maryland's lead, introducing bills and passing laws that restricted employer access to employee or applicant social media profiles.[86] United States Senators Charles Schumer and Richard Blumenthal further pioneered the password-protection cause, issuing open letters to the Equal Employment Opportunity Commission (EEOC) and the United States Department of Justice (DOJ) to determine the potential federal antidiscrimination, fraud, or privacy implications of the practice.[87] Senator Schumer decried the invasive practice, equating it to requesting house keys or access to personal diaries.[88] Confident that an investigation would demonstrate that the practice violates federal law, the Senators urged the DOJ and EEOC to investigate whether the practice violates the SCA or Computer Fraud and

83. Steinmetz, *supra* note 13 (explaining Collins's experience of employers demanding access to social media accounts).

84. *See* Aaron C. Davis, *Md. Corrections Department Suspends Facebook Policy for Prospective Hires*, WASH. POST (Feb. 22, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207486.html, *archived at* http://perma.cc/H8C3-ST4G (detailing Collins's experience); *see also* ACLU Maryland, *Want a Job? Password, Please!*, YOUTUBE (Feb. 10, 2011), http://www.youtube.com/watch?v=bDaX5DTmbfY (detailing Collins's experience and personal opinions concerning DOC actions); Khaki, *supra* note 14 ("The ACLU believes that this is a gross violation of personal privacy because people are entitled to their private lives online just as they are offline."). Despite having his profile set to the highest privacy settings, the DOC interviewers were able to access Collins's personal information. *See* ACLU Maryland, *supra*. Collins expressed his belief that despite its intentions to detect gang affiliation among applicants, the DOC had crossed the line in seeking his private information that was otherwise protected from the general public. *See id*. *But cf.* Mollie Brunworth, Articles, *How Women Are Ruining Their Reputations Online: Privacy in the Internet Age*, 5 CHARLESTON L. REV. 581, 589 (2011) (suggesting students' naïveté ignoring potential consequences of posting personal information online); Zansberg & Fischer, *supra* note 8, at 26 (stating young social media users comfortable in publicly sharing personal information).

85. *See* Matthew D. Keiser, *Maryland Bans Employers From Asking for Facebook and Other Social Media Passwords*, 14 E-COMMERCE L. REP., no. 6, 2012, at 11 (reviewing details of Maryland password-protection law).

86. *See* James J. Rooney & Diane M. Pietraszewski, *Crackdown on Employers' Access of Employees' Private Social Media Sites*, 19 N.Y. EMP. L. LETTER, no. 5, 2012, at 5 (discussing introduction of social media legislation in New York); Gutterman, *supra* note 11 (noting California passed password-protection legislation).

87. *See* Rooney & Pietraszewski, *supra* note 86 (noting legislative action following response from state senators).

88. Press Release, Senators Richard Blumenthal & Chuck Schumer, *supra* note 14 ("Employers have no right to ask job applicants for their house keys or to read their diaries–why should they be able to ask them for their Facebook passwords and gain unwarranted access to a trove of private information . . . ?").

Abuse Act—which prohibits intentional access to a computer without authorization to obtain information—and strongly urged that both organizations issue formal legal opinions on the matter.[89]

C. The Scope of Password-Protection Bills and Legislation

While a majority of states are currently considering their own password-protection bills, several have successfully passed laws prohibiting the practice.[90] Password-protection legislation not only seeks to protect against demands for employee or applicant log-in information, but also prohibits alternative methods of electronic surveillance conducted by an employer.[91] Enacted and proposed legislation seeks to protect against practices like "shoulder surfing"—asking a job applicant to log on to his or her social media page while the employer looks over the candidate's shoulder—or requiring an applicant or employee to "friend" the employer on Facebook.[92] This type of social media monitoring most often occurs in highly regulated public agencies, and positions that require extensive public contact.[93]

1. Passed Legislation

The new state laws share many common features, including: definitions of social media, employee, employer, etc.; a ban on employer requests or

89. *See id.* (providing copy of Senators' letters). Senators Blumenthal and Schumer sought guidance on social media issues and expressed concern that demanding access to social media "may be unduly coercive and therefore constitute unauthorized access under both SCA and the CFAA." *Id*; *see also supra* Part II.A.2 (discussing SCA claims dealing with social media). In addition, the Senators feared potential discrimination claims resulting from employers who bypass employee privacy protection on social media, thereby uncovering information about an employee or applicant such as gender, marital status, age, religion, or sexual orientation that may become a pretext for discrimination. *See* Press Release, Senators Richard Blumenthal & Chuck Schumer, *supra* note 14 (stating potential discrimination concerns); *see also supra* Part II.A.4.c (reviewing discrimination issues with employer social media use).

90. *See supra* note 11 and accompanying text (noting status of state bills and laws regarding password protection); *see also* Greg Naylor & Tom Foley, *Should You Use Social Media When Making Employment Decisions?*, 19 IOWA EMP. L. LETTER, no. 1, 2012, at 4 (offering arguments for and against password-protection legislation). In defense of the legislation, Foley suggests that employer use of social media creates a "potential gold mine for creative plaintiffs' lawyers" when employees are terminated based on their online activity. *Id.* On the contrary, one may argue that "honest" surfing serves legitimate business purposes and does have its place in a climate of growing social media. *See id*. *But see* 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, 146 (2013) (suggesting problems in enforcing password-protection legislation).

91. *See* Cooper, *supra* note 11 (explaining methods employers may exploit to gain access to employee social media); *see also* Naito, *supra* note 26, at 864 (noting innovative employer methods of monitoring employee computer activity). Employers may implement "flagging" software, which screens employee communications for certain words or phrases, or "keystroke logging," which allows an employer to track what an employee views or types on the computer. *See* Naito, *supra* note 26, at 864. Employers can use keystroke logging to obtain employees' passwords to social media sites when employees access those sites in the workplace. *See id.*

92. *See* Cooper, *supra* note 11 (discussing online screening practices).

93. *See id.* (noting prevalence of password requests in public work or to prevent conflicts of interest).

demands for passwords or access to social media accounts; a bar on adverse action or retaliation by the employer for employee refusal to acquiesce; and a list of exceptions to the general prohibition.[94] While legislators overall seek to eradicate social media harm, these laws provide varying degrees of protection to an employee or applicant's online presence.[95] For example, password-protection in Illinois extends to an employee's "account or profile on a social networking website" but explicitly excludes employee email.[96] Subtle language distinctions also differentiate the scope of each state's individual laws.[97] While each state prohibits demands, requirements, or requests for disclosure, states prohibiting "other means for accessing a personal account or service" leave greater room for interpretation.[98] Michigan addresses the issue by prohibiting employers from requiring an employee to "allow observation of" his varied social media activity, whereas Oregon explicitly forbids shoulder-surfing activity and requiring employees to "friend" employers.[99] The

94. *See* 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 LAW (June 10, 2014), http://www.bna.com/new-state-laws-restricting-employer-access-to-employees-personal-social-media-accounts/, *archived at* http://perma.cc/LSC2-5AMQ (listing common features among state password-protection laws).

95. *See id.* (noting "important differences among . . . new state laws"); *see also* Buckley, *supra* note 19, at 884 (observing varying degrees of inclusiveness among state password-protection laws); *cf.* Gary Gansale et al., *No Password for You: California Enacts Social Media Privacy Laws Affecting Employers and Postsecondary Educational Institutions*, 17 CYBERSPACE LAW., no. 10, 2012, at 1 (explaining California laws providing password protection to employers and postsecondary students); 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, 520-21 (2013) (citing password-protection laws affording students similar protection from academic institutions).

96. The Right to Privacy in the Workplace Act, §10, 820 ILL. COMP. STAT. 55/10(b) (2014) (declaring limits and expectations of employee privacy over social media in workplace); *see also* Prywes & Valdetero, *supra* note 94 (stating general state practice of extending protection to email outside of Illinois); Buckley, *supra* note 19, at 886 (describing Illinois's explicit exclusion of email from "social networking website" definition as curious).

97. *See* Buckley, *supra* note 19, at 885-86 (suggesting distinctions between state statutory language creates differing expectations of employee privacy); *see also* MD. CODE ANN., LAB & EMPL. § 3-712(b)(1) (West 2015) ("[A]n employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device."); Internet Privacy Protection Act, § 3, MICH. COMP. LAWS § 37.273 (2015) (stating employer prohibited from accessing or observing employee "personal internet account").

98. *See* MD. CODE. ANN., LAB. & EMPL. § 3-712(b) (West 2015) (stating employer prohibitions on various forms of password or username demands from employees); *see also* Buckley, *supra* note 19, at 887 (doubting whether Maryland's statute adequately prohibit compelled disclosure). Buckley emphasizes that all techniques of obtaining password-protected employee information should be addressed by statute. *See* Buckley, *supra* note 19 at 887.

99. MICH. COMP. LAWS § 37.273 (2015) (including "allow observation of" in prohibited requests employer may make on employee regarding social media); *see also* OR. REV. STAT. § 659A.330 (2014) (listing unlawful employment practices). Oregon's statutory language explicitly prohibits: requiring an employee or applicant to disclose or provide access to a social media account; compelling an employee or applicant to add the employer to a "list of contacts associated with a social media website"; or compelling an employee to access his or her social media site "in the presence of the employer and in a manner that enables the employer to view the contents of the personal social media account that are visible only when the . . . account is accessed

language of these state laws endeavors to protect against the same employer practices, but the laws' inconsistencies create a "complex patchwork" of laws of varying scopes.[100]

States also vary within the scope of recognized exceptions where employers *can* access an employee's personal accounts.[101] Although most states allow employer investigations into employee misconduct where the employer independently obtained information relating to it, the exception's threshold differs among states, requiring the employer's "reasonable belief" of misconduct in some states, but possession of "specific information" of employee misconduct in others.[102] Many states also created exceptions where federal or state law requires that companies screen and monitor employees, such as the Financial Industry Regulatory Authority (FINRA).[103] While some states explicitly exempted such regulatory agencies, others only allow employers access to personal information *after* the employer receives other information regarding employee misconduct.[104] Additionally, an employer often retains the right to access communications available to the public, or communications on the employer's system or devices.[105] The variations and

by the account holder's user name and password." OR. REV. STAT. § 659A.330 (1)(a)-(c).

100. *See* Woodrow Hartzog, *Social Data*, 74 OHIO ST. L.J. 995, 1009 (2013) (arguing inconsistencies in social media laws across jurisdictions create difficulty in adequately responding to issue). *See generally* Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 J. HIGH TECH. L. 42 (2014) (examining distinctions in language and restrictions among states' currently enacted password-protection legislation).

101. *See* Prywes & Valdetero, *supra* note 94 (expanding on exceptions to social media protection).

102. *See id.* (discussing variations among state law exceptions regarding investigations into employee misconduct); *see also, e.g.*, ARK. CODE ANN. § 11-2-124 (West 2014) (requiring employer possess "reasonabl[e] belie[f]" of misconduct to investigate employee social media account); MD. CODE ANN., LAB & EMPL. § 3-712(e)(2) (West 2015) (permitting employer investigation into employee Internet activity in "receipt of information" regarding unauthorized employee acts); UTAH CODE ANN. § 34-48-202(1)(c) (West 2014) (requiring employer possess "specific information" to conduct investigation into employee accounts).

103. *See* Prywes & Valdetero, *supra* note 94 (noting FINRA concern over social media laws interfering with duties). The self-regulatory body encouraged states to accept FINRA and allow FINRA representatives to dutifully monitor their representatives because FINRA representatives often communicate with customers through personal social media accounts. *See id.*; *see also* Stephen Joyce, *FINRA, Regulators Push Back on Bills Limiting Employer Social Media Access*, 18 ELECTRONIC COM. & L. REP. 917 (2013) (stating FINRA responded to legislators urging exemption of securities firms from social media laws).

104. *See* Prywes & Valdetero, *supra* note 94 (listing Arkansas, Michigan, Oregon, Utah, and Washington as compliant with FINRA); *see also* WASH. REV. CODE § 49.44.200(3)(c) (2015) (stating protection does not prevent employer from complying with state or federal statutes and regulations). *But see* MD. CODE. ANN., LAB & EMPL. § 3-712(e)(1) (West 2015) (requiring "receipt of information" before investigation into compliance with securities or financial law commences).

105. *See, e.g.*, The Right to Privacy in the Workplace Act, § 10, 820 ILL. COMP. STAT. 55/10(b)(3) (West 2014) ("Nothing in this subsection shall prohibit an employer from obtaining . . . information that is in the public domain."); MICH. COMP. LAWS § 37.273 (2015) (allowing employer access to information on employer owned or provided electronic equipment); OR. REV. STAT. § 659A.330(5) (2014) ("Nothing in this section prohibits an employer from accessing information available to the public."); UTAH CODE ANN. § 34-48-202 (West 2014) (allowing employer to monitor, review, access, or block data stored on device supplied by employer).

exceptions in the enacted laws demonstrate potential "gaps and loopholes for circumvention" that demand legislative attention.[106]

2. Pending Legislation

Although several states have successfully passed laws restricting employer requests for social media account information, the federal government and many other states are still working to implement similar laws.[107] Such bills are not without opposition.[108] In 2012, Congress introduced two similar bills, the Password Protection Act of 2012 (PPA) and the Social Networking Online Protection Act (SNOPA), both of which died early on.[109] The House reintroduced SNOPA in 2013 to prohibit an employer or institution of higher education from requesting usernames or passwords to email or social networking accounts, or retaliating where an employee, applicant, or student refuses to disclose such information; the bill does not, however list any exceptions to this prohibition.[110] SNOPA provides civil remedies as well as equitable relief.[111] The Senate's 2013 PPA bill similarly restricts employer coercion of or retaliation against employees under a civil penalty, but it does not prohibit similar acts by educational institutions.[112] The PPA does, however, include exceptions permitting an employer to access employee social media

106. *See* Poore, *supra* note 95, at 508-09 (commending state progress on social media bills while noting shortcomings). Enacting federal legislation may alleviate the discrepancies and loopholes that currently exist amongst state password-protection laws. *See id.* (advocating for federal password-protection legislation).

107. *See* Gesina M. Seiler, *Federal Law Introduced To Protect Employees' Facebook Accounts*, 21 WIS. EMP. L. LETTER, no. 7, 2012, at 3 (noting introduction of legislation in federal government and numerous states protecting employee personal social media). Both the House and Senate introduced bills intending to prohibit an employer from "compelling" an employee to provide access to a "protected computer." *See id.* (reviewing action in Senate and House of Representatives).

108. *See* 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, 730-40 (2013) (reviewing opposition rationale to bill). In Georgia, opponents of the bill believe that sufficient legislation already exists to combat employer social media password requests in Georgia. *See id.* at 733-34 (arguing SCA, NLRA, Title VII, and CFAA adequately protect employees). Furthermore, opponents argue that newly introduced federal legislation may preempt the state's action, rendering the bill unnecessary. *See id.* at 738. Opponents also emphasize an employer's need to properly investigate applicants in order to avoid negligent hiring. *See id.* at 730-31 (noting risks to employer).

109. *See* Buckley, *supra* note 19, at 884 (discussing introduction and failure of federal social networking bills in 2012).

110. *See* Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013) (prohibiting employers and "certain other entities" from requesting or demanding access to social media accounts); *see also* Lorene D. Park, *Social Media Melee: State Laws Gain Steam, Feds May Follow, New Issues Emerge*, WOLTERS KLUWER, http://www.employmentlawdaily.com/index.php/news/social-media-melee-state-laws-gain-steamfeds-may-follow-new-issues-emerge/ (last visited Mar. 30, 2015), *archived at* http://perma.cc/6P8A-3FHS (discussing federal social networking law "around the corner").

111. *See* Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013) (enforcing bill through civil penalties or injunctive actions). Civil penalties may not exceed $10,000. *See id.*

112. Password Protection Act of 2013, S. 1426, 113th Cong. (2013) (prohibiting employer access to or demands for employee information on a protected computer).

information in order to ensure compliance with federal or state laws and regulations or where an employer has "reasonable grounds to believe that the information sought . . . is relevant and material to protecting . . . intellectual property, a trade secret, or confidential business information."[113] Advocates for password-protection legislation suggest that comprehensive federal laws best combat employers' password-seeking practices.[114]

III. ANALYSIS

The current legislative framework unnecessarily complicates the employer and employee relationship with regard to social media.[115] Not only do employees already derive sufficient protection of their Internet personas from a number of statutory and common law measures, but employers also require latitude to defend against liability.[116] Individual state action does little to solve the issue at hand.[117] Where employees lack protection, the remedy should come from uniform federal legislation protecting employee passwords, clear employee social media policies, and employee self-regulation.[118]

A. Risk to Employees Is Minimal

Despite the urgency and fervor that seems to accompany state password-protection initiatives, little suggests that employer password requests are a widespread issue.[119] No clear statistics reveal that password requests actually threaten employees; many employers fear the lawsuits that would

113. *Id.* § 2(d)(2) (listing exceptions to general prohibition).

114. *See* Poore, *supra* note 95, at 525 (urging Congress to pass "a comprehensive solution" to password-protection problem); Buckley, *supra* note 19, at 890 (suggesting federal password protection will "supplement and improve existing laws"); *see also* Hartzog, *supra* note 100, at 1009 (claiming state laws create difficulty in establishing uniform social media policies). "The inconsistencies between [state] laws make clear the need to articulate a set of commonly held values to guide policy and self-regulatory efforts." Hartzog, *supra* note 100, at 1009.

115. *See infra* Part III.A-D (demonstrating outstanding issues related to current attempts at password protection); *see also* Hartzog, *supra* note 100, at 1009 (emphasizing inconsistencies between current state laws); Lario, *supra* note 90 at 146-50 (noting problems with current legislation). Lario asserts that the bills and laws lack a method of enforcement, preemptively assume that there is a problem with social media password requests, and ignore claims available to an aggrieved employee. *See* Lario, *supra* note 90, at 145-46.

116. *See supra* Part II.A (examining potential claims under U.S. Constitution, SCA, NLRA, and other statutory or common law measures); Shea, *supra* note 19 (sympathizing with employer need to combat against application fraud and negligent hiring claims).

117. *See infra* Part III.C (asserting gaps and lack of uniformity in state legislation leave ambiguity for employees lacking protection). Federal password protection would comprehensively protect employees in addition to the claims already at their disposal. *See id.* "Careful drafting and precise statutory terminology will provide effective and measured relief . . . ." Buckley, *supra* note 19, at 890.

118. *See infra* Part III.D (suggesting effective methods of navigating proper conduct on social media).

119. *See* Steinmetz, *supra* note 13 (suggesting employee password requests not common practice). "These [password-protection bill] proposals have spread at lightning speed despite a dearth of data about how many employers or school administrators out there are actually demanding access to Facebook pages or Twitter feeds." *Id.*

accompany such a practice and dare not make such a request.[120] News reports suggest that the "little-known practice" was in its infancy before gaining notoriety from the Maryland DOC case.[121] Although few employers may be requesting passwords in reality, the backlash prompted states to act quickly and halt the practice where it potentially never began.[122]

While states with enacted social media legislation attempt to further and explicitly protect employees from potential social media threats, adequate legal remedies already protect employees.[123] While acts like the SCA and NLRA were not specifically drafted with Facebook in mind, subsequent amendments and interpretations adequately adjust the legislation to the present-day technological landscape.[124] One may argue that such legislative action does not sufficiently account for modern innovations, but states' individual efforts to protect its employees are not without confusion or ambiguity in their wake.[125] Both the present protections and probable enactment of federal legislation in the future lessens the urgency and fervor with which states should currently pursue employee protection.[126]

120. *See* Lario, *supra* note 90, at 161 (claiming ineffectiveness of online privacy legislation and lack of data to support its advancement).

121. *See* Davis, *supra* note 84 (explaining Maryland DOC action called attention to Facebook password requests).

122. *See* Cooper, *supra* note 11 (suggesting few employers actually request passwords). "To place the controversy in context, asking for passwords is just the latest and perhaps most intrusive method employers *could* use to screen candidates using the Internet." *Id.* (emphasis added); *see also* Blanke, *supra* note 100, at 45 (asserting state legislative action as effort to "nip this growing practice in the bud").

123. *See* Determann, *supra* note 9, at 25 ("Existing rules can be and are . . . continuously applied to new technological, economic, and social developments"); *see also supra* Part II.A (reviewing current statutes and common law causes of action applicable to employee social media protection).

124. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980-81 (C.D. Cal. 2010) (determining private Facebook messages qualify under SCA protection); Pietrylo v. Hillstone Rest. Grp., No. 06-5757(FSH), 2009 WL 3128420, *3 (D.N.J., Sept. 25, 2009) (protecting coworker under SCA against coerced authorization to employee Facebook page); South, *supra* note 108, at 735 (explaining SCA and CFAA protection for coerced employees and applicants); *see also* Cilliers, *supra* note 8, at 574 (noting NLRA recognition of social media's integral role in workplace); Crane, *supra* note 4, at 672 (emphasizing SCA as well-suited solution to employer and employee issues).

125. *See* Baker, *supra* note 17, at 116 (arguing "inaction has led to obsolescence" of SCA). Cases consider whether current technology will guide courts in the future, but ultimately, Baker asserts, the legislature is tasked with updating the law in accordance with technology. *See id. See generally* Blanke, *supra* note 100 (discussing distinctions in language, restrictions, and permissions among states with password-protection legislation).

126. *See* South, *supra* note 108, at 734 (suggesting employees already have potential claims against employers accessing or monitoring their social media); Buckley, *supra* note 19, at 890 (asserting federal legislation will supplement and improve existing legislative scheme). "[S]ituations where employers request social media passwords and usernames, could potentially implicate the SCA, the CFAA, . . . the NLRA . . . [or] the privacy tort of intrusion of seclusion." South, *supra* note 108, at 734; *see also supra* Part II.C.2 (discussing attempts at federal legislation for employee social media protection in SNOPA and PPA).

B. Emphasis on Employee Protection Tends To Disregard Legitimate Employer Concerns

This recent surge in legislation does not necessarily balance the employee's right to privacy in social media with an employer's legitimate need to monitor employee activity.[127] Consider Robert Collins; although the Maryland DOC searched through his private Facebook messages, it was also doing its best to ensure against the disastrous consequences that might follow if the DOC inadvertently hired (or rehired) someone with gang affiliations.[128] While the Maryland DOC arguably overstepped its boundaries in that instance, employers do require some means to protect trade secrets, investigate employee misconduct, prevent negligent hiring, and ensure compliance with statutory regulations.[129] Much proposed and enacted legislation accounts for these needs, but some only provide recourse after it may be too late for the employer, and set the standard too high for when intervention is considered appropriate.[130] Moreover, the distinct language of each state's statutes creates confusion over what action is appropriate, especially for employers acting across multiple states.[131] The addition of state password-protection legislation adds confusion to the complex framework that already attempts to dictate proper employer interaction with employee social media behavior.[132]

127. *See* Determann, *supra* note 9, at 26 (noting employer use of social media for collaboration, marketing, and to "mitigate against risks"). Employer concerns include the "risks" involved with "trade secret disclosures, losses of productivity, violations of anti-spam laws, harassment of co-workers, third party copyright infringements, illegal endorsements," and employee misconduct. *Id.* *But see* Shea, *supra* note 19 (asserting risks associated with snooping outweigh risk to employer).

128. *See supra* note 84 and accompanying text (discussing Maryland DOC action regarding Robert Collins and DOC's motivation behind practice); *see also* Steinmetz, *supra* note 13 (noting Maryland authorized practice to combat gang violence in state's prison system).

129. *See* Mello, *supra* note 4 (explaining modes of and need for traditional employer monitoring). An employer might monitor employee conduct to ensure productivity and prevent employees from engaging in personal business. *See id.* An employer also needs to protect its confidential documents, files, and information from dissemination at the hands of a disgruntled employee. *See id.*; Naito, *supra* note 26, at 861-66 (discussing employer need to protect interests and shield against liability). Employers must be mindful of liability in the case of coworker harassment or defamation, where social media diligence would place the employer in a position in which he would or should have known about the activity. *See* Naito, *supra* note 26, at 861-63; *see also* Shea, *supra* note 19 (suggesting application fraud may subject employer to negligent hiring claims); South, *supra* note 108, at 739 (noting employer need to protect against negligent hiring); ACLU Maryland, *supra* note 84 (detailing Collins's opinion Maryland DOC crossed line in demanding social media passwords).

130. *See supra* note 105 and accompanying text (noting differences among enacted legislation for when employers may intervene to assure securities compliance). Whereas Arkansas, Michigan, Oregon, Utah, and Washington are considered compliant with FINRA, Maryland requires the "receipt of information" before an employer may investigate an employee's compliance with securities or financial law. *See id.*

131. *See* Hartzog, *supra* note 100, at 1008 (asserting no "common guidance" exists to direct privacy protections). Although many states have passed social media legislation, states do not always use identical or similar terms. *See id.* at 1009. A set of "commonly held values" must guide policy and self-regulation because each state has its own terms (some undefined), its own scope of coverage, and its own remedies. *See id.*; *see also* South, *supra* note 108, at 739 (summarizing opposition to state legislation in Georgia); *supra* Part II.C.1 (noting distinctions between states in prohibitions and permissions for social media legislation).

132. *See supra* Part II.A (explaining statutory protections available to protect employee social media);

C. Federal Legislation Will More Successfully Resolve the Issue

State password-protection laws both duplicate and confuse the efforts of currently existing measures protecting employees' use of social media.[133] If new legislation ought to be passed, however, then a federal password-protection law would resolve the complexity and loopholes that state password-protection legislation have created.[134] State laws appeal to the public's reactionary demand for action against the invasive practice of some employers, but fail to provide a comprehensive, long-term solution because each state's laws vary widely in language, degree of protection, and scope of employer rights.[135]

Federal legislation would fill the gaps that state laws leave unanswered.[136] States are acting as laboratories for password-protection laws—whether states ought to or not—and thus, federal legislators will have the opportunity to assess what provisions work and what is best left alone.[137] If the combined protections of the NLRA, SCA, and other provisions do not adequately account for the growing and changing technological landscape, then employers and employees deserve a federal uniform approach that defines what role social media plays in the professional world.[138]

supra note 105 (noting distinctions between states' legislation complicates successful recognition of desired employee protection).

133. *See* Hartzog, *supra* note 100, at 1009 (stating laws create "complex patchwork" complicating social media policy-making for multi-state employers). *See generally* Sherman, *supra* note 9 (expressing varied concerns employer must consider for acceptable social media policy). Employers must take care to ensure, per NLRA regulations that their social media policies are not overbroad, that hiring decisions are not negligent or uninformed, and that any research conducted on employees or applicants is thoroughly documented. *See* Sherman, *supra* note 9; *see also* South, *supra* note 108, at 739 (claiming state legislation will limit business and employer protection and create unnecessary legislation).

134. *See* Buckley, *supra* note 19, at 890 (advocating for federal password-protection legislation). "Federal password protection legislation would serve to supplement and improve existing laws pertaining to protection of stored wire and electronic communications, unauthorized access, and employment discrimination, while promoting a healthy public forum for important discourse on social media websites by students and employees." *Id.*

135. *See* Blanke, *supra* note 100, at 45 (noting state legislative response attempting to nip password request practice "in the bud"); Poore, *supra* note 95, at 508-09 (asserting state efforts laudable, but leave "gaps and loopholes for circumvention"); South, *supra* note 108, at 734 (indicating pending federal legislation addresses issue and protects employees where state laws fail); Steinmetz, *supra* note 13 (asserting proposals for state legislation spread "at lightning speed"); *see also* Zansberg & Fischer, *supra* note 8, at 25-26 (suggesting older generation less likely to perceive their personal information online as public).

136. *See* Poore, *supra* note 95, at 509 (suggesting state legislation leaves gaps and unaddressed loopholes); *supra* note 133 and accompanying text (describing faults of state law).

137. *See* Blanke, *supra* note 100, at 80 (suggesting state legislation allows states to act as laboratories and provide model for others); Buckley, *supra* note 19, at 890 (advocating federal legislators use state acts as guide). Through their efforts, state legislators can aid federal lawmakers in drafting their own legislation that balances employee protection without being "overly board or under-inclusive." Buckley, *supra* note 19, at 890.

138. *See* Poore, *supra* note 95, at 526-27 (arguing emerging technological issues require new federal legislation). Just as Congress passed the EPCA in 1986, the call for federal password protection of social media requires comprehensive legislation that will "keep pace with ever-changing technology." *Id.* at 526; *see also supra* notes 124-25 and accompanying text (suggesting federal legislation or current statutory protections

D. Best Practices

Despite the arguments against state password-protection legislation, the thirty-five states that have either enacted or are currently considering such laws demonstrate its inevitability.[139] Even states with enacted legislation will need time to determine—and will likely encounter litigation over—the meaning of "social networking website," "personal internet account," or "to gain access to" before employers and employees may confidently navigate what constitutes appropriate action on social media.[140] Although federal legislation may eliminate some of the current complexity, both employers and employees or applicants are still likely to face uncertainty under password-protection laws while federal and state legislators draft and develop solutions.[141]

In the meantime, federal *or* state password-protection legislation is not necessarily the best or strongest tool at an employer's, employee's, or applicant's disposal.[142] First, should an employer improperly demand access to employee social media, employees should be aware of the protections available to them, even in states without enacted password-protection legislation.[143] Second, employers should have comprehensive and clear social media policies that do not run afoul of the NLRA; explicit provisions and policies may eliminate much of the uncertainty in the workplace over social media that password-protection legislation seeks to resolve.[144] Third, and perhaps most

best protects employees and employer social media relationship).

139. *See supra* notes 11-12 and accompanying text (noting states considering or enacting password-protection laws in 2012-2013).

140. *See* Blanke, *supra* note 100, at 55-71 (explaining distinctions in language between state laws restricting employer access to social media). For example, California's law prohibits an employer from requiring or requesting that an employee or applicant disclose his or her username or password, but it also prohibits an employer from requesting or requiring an employee or applicant to access his social media in front of the employer. *See id.* at 63. Other states—Arkansas, Colorado, Oregon, and Washington—employ similar language to California, but also restrict an employee from having to add an employer or supervisor to his social media list of contacts or friends. *See id.* at 57. Vermont arguably has the strongest protections because it prohibits an employer from taking action that allows access to information generally unavailable to the public. *See id.* (demonstrating distinctions between statutory language). Such distinctions may create varying rights for employees across states and do not clearly define how employers, especially a multi-state employer, ought to act in certain contexts. *See* Hartzog, *supra* note 100, at 1009 (describing difficulties for multi-state employers determining appropriate social media action).

141. *See supra* Part III.C (asserting federal legislation will eliminate some complexity of password-protection laws). *See generally* Blanke, *supra* note 100 (demonstrating distinctions among states' social-media legislative language).

142. *See supra* Part III.C (arguing clear social media policies best protect employer and employee rights).

143. *See supra* Part II.A (describing protection afforded by Constitution, SCA, NLRA, privacy torts, discrimination claims, and off-duty conduct statutes).

144. *See* Whitfield, *supra* note 20, at 874-77 (proposing suggestions for coherent social-media policies). An employer may wish to consult legal counsel in drafting a social media policy in order to avoid enforceability issues and balance an employer's business interests with an employee's privacy. *See id.* at 874-75. A successful policy should: specify what constitutes appropriate employee use of social media and sanctions for noncompliance, establish who owns the social media account on work devices, unambiguously define violations, avoid "chilling" an employee's rights under the NLRA, and update policies in accordance

importantly, employees must use good sense to self-regulate social media activity—once information is put into cyberspace, it may prove difficult to erase or control.[145]

IV. CONCLUSION

Social media has drastically changed the way individuals work, play, and communicate. There is no sense in avoiding technology, but employers, employees, students, and applicants—everyone—must use common sense before posting, blogging, tweeting, friending, or checking up on someone else's activity. State password-protection legislation attempts to protect against more egregious invasions into an employee's social media persona but haphazardly affords employees varying levels of protection and recourse depending on where they live. Both employers and employees must recognize employee social-media protections that already exist, as well as the power of self-regulation and effective social media policies. As social media's relevance in the workplace expands, employees may sleep better at night under password-protection legislation, but the best policy is for employees and employers alike to think before sending, clicking, or checking.

Brittanee L. Friedman

with the growth of technology. *See id.* at 875-77; *see also* Mahoney, *supra* note 20, at 31 ("[W]ell-defined social media polic[ies] today can help reduce . . . an employer's risks tomorrow."); *supra* Part II.A.3 (demonstrating how NLRA policies protect employees from overly broad or vague social media policies).

145. *See* Abril et al., *supra* note 7, at 108 ("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[.]"); Brunworth, *supra* note 84, at 582 (stating women post behavior online "that would shock prior generations"). Individuals perhaps do not realize how social media posts may damage their long-term reputation irreparably. *See* Brunworth, *supra* note 84, at 583-88; Determann, *supra* note 9, at 18 (arguing individual "right to be forgotten" is myth in United States); *see also* Clifford, *supra* note 9 (reporting employee damaged Domino's reputation in posting video tampering with food as joke).