5-1-2014

Employers Can't Request Your Social Media Passwords, But You Can't Sue: The Need for a Private Right of Action in New Jersey's Social Media Legislation

Amy Christine Gromek

Employers Can't Request Your Social Media Passwords, But You Can't Sue: The Need for a Private Right of Action in New Jersey's Social Media Legislation

Amy C. Gromek

I. Introduction

When Justin Bassett, a New York City-based statistician, interviewed for a new job, he was confronted with one request he did not expect: to turn over his Facebook username and password.[1] Bassett had answered a few character questions when the interviewer turned to her computer to search for his Facebook profile.[2] The interviewer could not see Bassett's profile, however, because the setting was "private."[3] She turned back to him and asked him to hand over his login information.[4] Bassett refused to do so and withdrew his application, stating that he did not want to work for a company that would seek such personal information.[5]

Similarly, Maryland corrections officer Robert Collins was disturbed when he was required to provide his Facebook login and password to the Maryland Division of Corrections ("DOC") during a recertification interview.[6] Collins sat in the interview while

---

[1] Shannon Mcfarland, *Job Seekers Getting Asked for Facebook Passwords*, USATODAY.COM, Mar. 21, 2012, http://usatoday30.usatoday.com/tech/news/story/2012-03-20/job-applicants-facebook/53665606/1.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] Meredith Curtis, *Want a Job? Password, Please!*, ACLU BLOG OF RIGHTS (Feb. 18, 2011, 2:04 pm), https://www.aclu.org/blog/technology-and-liberty/want-job-password-please.

the interviewer logged on to his account and read his postings and those of his family and friends.[7] Reflecting on the interview, Collins said, "[W]hat was not customary and usual was a request, or to me rather a demand, you know, which was the insinuation for my Facebook e-mail and login information. My personal login information."[8] Collins later filed a complaint with the American Civil Liberties Union ("ACLU") of Maryland.[9]

These instances, along with others publicized in the media,[10] illustrate the efforts that some employers have taken in recent years to vet prospective and current employees. With the rise of social networking, it has become increasingly common for employers to review prospective employees' *publicly* available social media accounts, including Facebook profiles and Twitter pages, to learn more about them as job candidates.[11] In fact, according to a 2012 study conducted by CareerBuilder,[12] thirty-seven percent of companies use social networking sites to research job candidates. [13] Nevertheless, those Facebook users who set their profiles to the "private" setting may now be asked by employers to hand over their

[7] *Id.*
[8] *Want a Job? Password, Please!*, YOUTUBE, http://www.youtube.com/watch?v=bDaX5DTmbfY (last visited Dec. 3, 2013).
[9] Bob Sullivan, *Gov't Agencies, Colleges Demand Applicants' Facebook Passwords*, NBCNEWS.COM, Mar. 6, 2012, http://www.nbcnews.com/technology/govt-agencies-colleges-demand-applicants-facebook-passwords-328791.
[10] *See* Matt Gouras, *Montana City Asks Job Applicants For Facebook Passwords*, HUFFINGTON POST, Jun. 19, 2009, http://www.huffingtonpost.com/2009/06/19/montana-city-asks-job-app_n_218152.html (explaining how criticism prompted a Montana city to drop its request that government job applicants turn over their usernames and passwords to Internet social networking and Web groups).
[11] Mcfarland, *supra* note 1.
[12] CareerBuilder maintains a website devoted to "human capital solutions." *About Us*, CAREERBUILDER.COM, http://www.careerbuilder.com/share/AboutUs/default.aspx (last visited Oct. 17, 2013).
[13] Press Release, PR Newswire, Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey (Apr. 18, 2012), *available at* http://www.prnewswire.com/news-releases/thirty-seven-percent-of-companies-use-social-networks-to-research-potential-job-candidates-according-to-new-careerbuilder-survey-147885445.html.

Facebook usernames and passwords, a practice that critics are calling "'an egregious privacy violation.'"[14]

The Stored Communications Act ("SCA")[15] and the Computer Fraud and Abuse Act ("CFAA")[16] are federal laws that may provide some protections in this context, though the extent of these protections remains unclear. There have been attempts in Congress to pass other federal legislation that would provide greater legal protection for employees with regard to their private social networking accounts, including the Social Networking Online Protection Act ("SNOPA"),[17] the Password Protection Act ("PPA"),[18] and an amendment to the Cyber Intelligence Sharing and Protection Act ("CISPA").[19] These laws have failed to pass in Congress, however.[20] Nevertheless, several states now have pending or enacted state legislation to address this issue.[21] On August 28, 2013, New Jersey's employment-related social media bill was signed into law,[22] making it the thirteenth state in the nation to have enacted legislation in this area.[23]

Part II of this Comment will explore employers' and employees' views on social media login and password requests in the employment setting and Facebook's own policy

[14] Mcfarland, *supra* note 1.
[15] Stored Communications Act, 18 U.S.C. § 2701 et seq. (2013).
[16] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2013).
[17] Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).
[18] Password Protection Act, H.R. 5684, 112th Cong. (2012).
[19] Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).
[20] *See infra* notes 84, 87, 90.
[21] *See Employer Access to Social Media Usernames and Passwords 2013*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last visited Dec. 3, 2013).
[22] *Id.*
[23] The states that have enacted employment-related legislation thus far include Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and Washington. *See Employer Access to Social Media Usernames and Passwords 2013*, *supra* note 21; Employer *Access to Social Media Usernames and Passwords 2012*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx (last visited Dec. 3, 2013).

given the potential proliferation of this trend. Part III will examine both federal and state attempts at a remedy and analyze the effectiveness of each initiative. Part IV will trace the legislative history of New Jersey's social media password law and highlight the provisions of the law as enacted. Finally, Part V will argue that, in order to effect true balance, New Jersey's law should be revised to include a private right of action with certain limitations. Part V will also introduce a draft for the proposed private right of action.

II. Background and Facebook's Policy Regarding Username and Password Inquiry

In examining the laws in effect regarding employers' use of employees' social media passwords, it is first necessary to consider both employer and employee views on the practice. Aside from allowing employers to screen prospective employees who have private profiles,[24] the practice also provides a way for employers to monitor current employees.[25] For example, if employers are permitted to ask for employees' social media passwords, they can investigate employees who they suspect are divulging proprietary information via social media channels.[26] Additionally, employers in the law enforcement field may justify asking for social media passwords by invoking a safety rationale.[27] An agency hiring prison guards, for instance, would likely want to search a potential employee's private social media profile for photos indicating any gang affiliation.[28] Moreover, scholars have pointed out that employers can be civilly liable for negligent hiring if they fail to uncover an obvious flaw in

[24] *See 37 Percent of Employers Use Facebook to Pre-Screen Applicants, New Study Says*, HUFFINGTON POST, Apr. 20, 2012, http://www.huffingtonpost.com/2012/04/20/employers-use-facebook-to-pre-screen-applicants_n_1441289.html.
[25] Duane Craig, *U.S. States Lining Up to Limit Employer Access to Personal Social Media Accounts*, TECHREPUBLIC (Jun. 17, 2013, 8:03 am), http://www.techrepublic.com/blog/social-media-in-the-enterprise/us-states-lining-up-to-limit-employer-access-to-personal-social-media-accounts/.
[26] *Id.*
[27] Sullivan, *supra* note 9.
[28] *Id.*

an employee's background or character and that an individual's social networking profile can "provide an accurate window into the individual's personality and character."[29]

By contrast, many employees and employee-side proponents have rejected employer justifications for this practice and voiced their concerns over its invasion of employees' privacy.[30] One employee of the Montana ACLU has likened the policy to employers "'saying they want to look at your love letters and your family photos[.]'"[31] Many critics think it "certainly crosses the privacy line" and emphasize that it is not just the employee's privacy that is invaded, but also the privacy of the employee's "connections."[32] Others note how in a difficult job market, "not many people are in a position to refuse" an employer's inquiry of this type.[33] Critics have cautioned that "private groups and profile[s] could reveal information employers could not legally base hiring decisions on, such as a person's religion[.]"[34] Furthermore, others have posited that employers' requests for social media information are unnecessary because employers can rely on background checks,[35] professional references, and public Internet searches when seeking more information about applicants and employees.[36]

While employers and employees have differing views of employers' potential practice of asking employees for social media usernames and passwords, Facebook itself has

---

[29] Alissa Del Riego et al., *Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy*, 16 NO. 3 J. INTERNET L. 1, 18 (2012).
[30] Gouras, *supra* note 10.
[31] *Id.*
[32] Gouras, *supra* note 10; Craig, *supra* note 25.
[33] *Employers, Don't Ask for Facebook Usernames and* Passwords, Editorial, N.J.COM, Mar. 20, 2012, http://blog.nj.com/njv_editorial_page/2012/03/employers_dont_ask_for_faceboo.html.
[34] Gouras, *supra* note 10.
[35] For a brief discussion of the Fair Credit Reporting Act and background checks, *see* note 52 *infra.*
[36] 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 (2013). In response to this argument, employers may counter that states are increasingly limiting employers' access to or ability to perform background checks. *See id.* at 732.

repudiated the practice, both in a public statement and its Statement of Rights and Responsibilities.[37] On March 23, 2012, Erin Egan, Chief Privacy Officer of Facebook, wrote a Facebook Note addressing the "distressing increase" in reports of employers seeking to gain access to people's Facebook profiles.[38] Egan stated the following:

> As a user, you shouldn't be forced to share your private information and communications just to get a job. And as the friend of a user, you shouldn't have to worry that your private information or communications will be revealed to someone you don't know and didn't intend to share with just because that user is looking for a job. That's why we've made it a violation of Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password . . . . We don't think employers should be asking prospective employees to provide their passwords because we don't think it's the right thing to do.[39]

Facebook's Statement of Rights and Responsibilities, as referenced by Egan, specifically states in its "Registration and Account Security" section, "You will not share your password . . . let anyone else access your account, or do anything else that might jeopardize the security of your account."[40] In its "Safety" section, the Statement of Rights and Responsibilities says, "You will not solicit login information or access an account belonging to someone else."[41] In sum, Facebook has sided with employees while essentially instructing them through its Statement of Rights and Responsibilities not to share their passwords.[42] While it is unclear what kind of legal significance these statements have,[43]

---

[37] *See Protecting Your Passwords and Your Privacy*, FACEBOOK, https://www.facebook.com/note.php?note_id=326598317390057 (last visited Oct. 17, 2013); *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last visited Oct. 17, 2013).
[38] *Protecting Your Passwords and Your Privacy*, *supra* note 37.
[39] *Id.*
[40] *Statement of Rights and Responsibilities*, *supra* note 37.
[41] *Id.*
[42] *Protecting Your Passwords and Your Privacy*, *supra* note 37.
[43] *See* Wendy McElroy, *When Did Facebook Become Congress?*, THE FUTURE OF FREEDOM FOUNDATION (Mar. 27, 2012), http://fff.org/explore-freedom/article/when-did-facebook-become-congress/ ("The most likely grounds for a lawsuit would be breach of contract . . . . The party most clearly in breach of the agreement would be the Facebook user, however, and not the employer. Understandably, Facebook has little interest in

there have been attempts to implement laws at both the federal and state levels that would increase protections for employees when it comes to their private social media accounts.[44] Part III will explore these efforts.

III. Federal and State Legislation Addressing Employer Requests for Employee Usernames and Passwords

Both the public and politicians have voiced concern over employer requests for social media passwords.[45] Although federal legislation has stalled regarding employers' inquiries into employees' social media passwords,[46] state laws have passed, albeit with varying protections.[47]

A. The Stored Communications Act ("SCA") and the Computer Fraud and Abuse Act ("CFAA")

In March 2012, U.S. Senators Richard Blumenthal (D-CT) and Charles E. Schumer (D-NY) asked the U.S. Equal Employment Opportunity Commission ("EEOC") and the U.S. Department of Justice ("DOJ") to investigate whether employers asking for Facebook

---

suing users, on whose goodwill it depends."). *See also* discussion *infra* in Part III.A regarding potential claims under the Computer Fraud and Abuse Act ("CFAA").

[44] *See* discussion in Part III *infra*.

[45] *See* Press Release, Senator Richard Blumenthal, Blumenthal, Schumer: 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), *available at* http://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-schumer-employer-demands-for-facebook-and-email-passwords-as-precondition-for-job-interviews-may-be-a-violation-of-federal-law-senators-ask-feds-to-investigate.

[46] *See* Joanna Stern, *Legislation Would Make it Illegal for Employers to Ask for Passwords*, ABC NEWS, Feb. 6, 2013, http://abcnews.go.com/Technology/snopa-law-make-illegal-employers-passwords-reintroduced-congress/story?id=18422329 (detailing the Social Networking Online Protection Act's death in Congress); Sara Gates, *CISPA Amendment Banning Employers From Asking For Facebook Passwords Blocked*, HUFFINGTON POST, Apr. 23, 2013, http://www.huffingtonpost.com/2013/04/21/cispa-amendment-facebook-passwords-blocked_n_3128507.html (explaining Congress's blockage of an amendment to the Cyber Intelligence Sharing and Protection Act).

[47] *See Employer Access to Social Media Usernames and Passwords 2013*, *supra* note 21.

passwords during job interviews are violating federal law.[48] According to the Associated Press, the Department of Justice regards it as a federal crime to enter a social networking site in violation of the terms of service, but during congressional testimony, the agency said such violations would not be prosecuted.[49] This Associated Press statement, however, pre-dated the senator's request for EEOC and DOJ investigation.[50] It does not appear that the DOJ or the EEOC responded to the senators' request.

In their letter to the DOJ,[51] the senators urged the DOJ to investigate whether this practice violates the Stored Communications Act ("SCA") or the Computer Fraud and Abuse Act ("CFAA").[52] The SCA creates criminal and civil liability for certain unauthorized access to stored communications and records.[53] The SCA states that whoever "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished[.]"[54] The

[48] Press Release, *supra* note 45.
[49] Mcfarland, *supra* note 1.
[50] *See* Mcfarland, *supra* note 1; Press Release, *supra* note 45.
[51] Press Release, *supra* note 45.
[52] *Id.* Notably, the Fair Credit Reporting Act ("FCRA") likely was not mentioned as a potentially relevant statute because the FCRA is implicated when a *consumer reporting agency* furnishes a "consumer report." 15 U.S.C. § 1681b (2013). A "consumer report" is a written, oral, or other communication by a consumer reporting agency that bears on several different factors and can be used in establishing a consumer's eligibility for employment purposes, among other things. § 1681a. *See* South, *supra* note 36, at 727. ("When employers directly ask employees for [their social media usernames and passwords], the FCRA will not apply and thus there is no violation of the FCRA."). Additionally, though the National Labor Relations Board has been active in recent years, its focus has generally been on employee speech on social media forums that qualifies as "concerted action." For more details, *see* Memorandum from Anne Purcell, Assoc. Gen. Counsel, National Labor Relations Board to All Regional Directors, Officers-in-Charge, and Resident Officers (Jan. 24, 2012).
[53] In re iPhone Application Litig., 844 F.Supp.2d 1040, 1056 (N.D. Cal. 2012), citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).
[54] 18 U.S.C. § 2701(a).

SCA creates a private right of action.[55] The SCA's general prohibitions in § 2701(a), however, do not apply "with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user[.]"[56]

Notably, there is case law to suggest that when supervisors request employee login credentials, and access otherwise private information with those credentials, that the employer may be subject to civil liability under the SCA.[57] In a District of New Jersey case, a restaurant employee, St. Jean, provided her MySpace.com login information to restaurant managers upon their request and the managers used her password multiple times to access the Spec-Tator, an invite-only chat group.[58] The Plaintiffs in the case, two other restaurant servers, claimed that the Defendant restaurant violated the SCA and emphasized that St. Jean's purported "authorization" was coerced.[59] The District of New Jersey found that there was sufficient evidence upon which the jury below could find a verdict for the Plaintiffs on their SCA claim.[60]

Similarly, in a case from the 9th Circuit, Konop, a pilot for Hawaiian Airlines, created and maintained a secured website where he posted bulletins that were critical of his employer.[61] Konop controlled access to his website by requiring visitors to log in with a username and password and maintaining a list of people who were eligible to access the

[55] § 2707.
[56] § 2701(c).
[57] *See* Press release, *supra* note 45.
[58] Pietrylo v. Hillstone Rest. Grp, No. 06-5754, 2009 WL 3128420, at *2–3 (D.N.J. Sept. 25, 2009).
[59] *Id.* at *3 (St. Jean testified that she felt she had to give her password to the manager because she worked at the restaurant and for the manager.).
[60] *Id.*
[61] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872 (9th Cir. 2002).

website.[62] Hawaiian Airline's vice president asked two other pilots for permission to use their names to access Konop's website and the pilots agreed.[63] On appeal, the 9th Circuit held that neither of the pilots were "users" of the website at the time they authorized the vice president to view it, as required by the § 2701(c)(2) exception.[64] Thus, the 9th Circuit reversed the district court's grant of summary judgment to Hawaiian Airlines on Konop's SCA claim.[65]

Pietrylo, in particular, provides hope for employees that when supervisors or managers ask for employee login credentials, and thereafter access otherwise private social media sites with those credentials, the employer may be subject to liability under the SCA. Though the facts in *Pietrylo* involved one employee providing her MySpace.com login information and an ensuing suit from two other employees,[66] the reasoning of the case may be directly applicable to the situation at hand. For instance, an employee could argue that in turning over his or her Facebook login to an employer who seeks to examine that employee's own profile, the employee does not "authorize"[67] the action but instead feels coerced to supply the information.[68] Given the lack of case law directly on point, however, it remains overall unclear what protections the SCA may provide for current employees in

---

[62] *Id.*
[63] *Id.* at 873.
[64] *Id.* at 880. Again, the § 2701(c) exception states that the SCA's general prohibitions in § 2701(a) do not apply "with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) *by a user of that service with respect to a communication of or intended for that user*" (emphasis added). § 2701(c).
[65] *Konop*, 302 F.3d at 880.
[66] *Pietrylo*, 2009 WL 3128420, at *2–3.
[67] *See* 18 U.S.C. § 2701(a).
[68] *See* Andrew M. Gould, *If You're Asking for the Facebook Passwords of Job Candidates, You're Asking for Trouble*, GPSOLO EREPORT (Aug. 2012), http://www.americanbar.org/publications/gpsolo_ereport/2012/august_2012/facebook_passwords_job_candidates_trouble.html.

this specific context.[69] Moreover, as Senators Blumenthal and Schumer pointed out in their letter to the DOJ, these cases involved current employees[70] and, thus, SCA protections for prospective employees are still undetermined as well.[71]

Senators Blumenthal and Schumer also asked the DOJ to investigate whether this practice violates the Computer Fraud and Abuse Act ("CFAA").[72] The CFAA is a federal statute that, among other things, creates liability for whoever "intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains . . . information from any protected computer."[73] In *United States v. Drew*, the court examined whether any conscious violation of an Internet website's terms of service will cause an individual's contact with the website via computer to become "intentionally access[ing] . . . without authorization" or "exceeding authorization."[74] The case involved a mother and daughter pair who set up a fictitious MySpace profile in violation of MySpace's terms of service.[75] The court first concluded that "intentional breach of the [MySpace terms of service] can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute."[76] However, the court ultimately held that basing a CFAA violation upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine, stating that individuals of

[69] *Id.* ("Whether requiring an individual to provide access to their Facebook page as a condition of employment constitutes sufficient authorization or coercion is unclear.").
[70] Press Release, *supra* note 45.
[71] For an interesting argument that an employer's direct "demand" or "request" to an employee or applicant for his or her login information does, indeed, violate the SCA, *see* Nicholas D. Beadle, *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, 402 (2012).
[72] Press Release, *supra* note 45
[73] 18 U.S.C. § 1030(a)(2)(C).
[74] U.S. v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009).
[75] *Id.* at 452.
[76] *Id.* at 461.

"common intelligence" are not on notice that a breach of a terms of service contract can become a crime under the CFAA.[77] Given this case law, it is seemingly unlikely that the CFAA would be much help in holding employers liable for violation of Facebook's Statement of Rights and Responsibilities when they solicit employee passwords.[78]

B. Other Attempts at Federal Legislation

Considering the uncertainty of what specific type of protections the SCA and the CFAA may provide to employees and prospective employees, congressional members have made other attempts to pass legislation concerning employers' requests for employees' social media passwords. The Social Networking Online Protection Act's ("SNOPA") most recent version was introduced in the House of Representatives on February 6, 2013.[79] The Act would make it unlawful for any employer "to require or request that an employee or applicant for employment provide the employer with a user name, password, or any other means for accessing . . . the personal account of the employee or applicant on any social networking website."[80] Also, among other things, the proposed law makes it unlawful to discharge or discipline any employee or applicant for employment because the employee or applicant for employment refuses or declines to provide a username or password.[81] This law, however, has not been successful in passing previously.[82] SNOPA was originally

[77] *Id.* at 464.
[78] *See* note 41 and accompanying discussion.
[79] Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013).
[80] *Id.* at § 2(1).
[81] *Id.* at § 2(2)(A).
[82] *See* Stern, *supra* note 46.

introduced in May 2012,[83] but died when Congress adjourned at the end of 2012.[84] It is likely that this year it will reach the same fate.[85]

The Password Protection Act ("PPA") was introduced in 2012 to "prohibit employers from compelling or coercing any person to authorize access to a protected computer, and for other purposes."[86] The Act died in Congress,[87] though it has been reintroduced this year.[88] Additionally, despite the passage in the House of Representatives of the broad cybersecurity bill, Cyber Intelligence Sharing and Protection Act ("CISPA")[89] this year, a last-minute amendment to the bill that would ban employers from requiring employees to reveal their social media passwords was blocked.[90] Overall, though there have been many attempts at federal legislation specifically addressing this issue, none have proved successful yet.[91]

C. Potential State-Law Remedies

Some legal scholars have advanced that state common law privacy protections may help in protecting employees from unwanted employer intrusions into their social media

[83] *See* Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).
[84] *Stern*, *supra* note 46.
[85] *See H.R. 537: Social Networking Online Protection Act*, GOVTRACK.US, https://www.govtrack.us/congress/bills/113/hr537 (last visited Nov. 23, 2013) (listing a prognosis of "0% chance of being enacted").
[86] Password Protection Act, H.R. 5684, 112th Cong. (2012).
[87] *H.R. 5684 (112th): Password Protection Act of 2012*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/hr5684#overview (last visited Oct. 18, 2013).
[88] Password Protection Act, H.R. 2077, 113th Cong. (2013).
[89] Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013).
[90] Gates, *supra* note 46; Eric B. Meyer, *Congress Blocks One Proposed Ban on Requesting Social Media Passwords*, TLNT (Apr. 24, 2013), http://www.tlnt.com/2013/04/24/congress-blocks-one-proposed-ban-on-requesting-social-media-passwords/.
[91] For a discussion of the shortcomings of the PPA and SNOPA, *see* Timothy J. Buckley, *Password Protection Now: An Elaboration on the Need for Federal Password Protection Legislation and Suggestions on How to Draft It*, 31 CARDOZO ARTS & ENT. L.J. 875, 884–89 (2013).

accounts.[92] In New Jersey, to state a claim for intrusion upon one's seclusion or private affairs, a plaintiff must allege sufficient facts to demonstrate that (1) her solitude, seclusion, or private affairs were intentionally infringed upon, and that (2) this infringement would highly offend a reasonable person.[93] *Ehling* involved a registered nurse and paramedic who alleged that Monmouth-Ocean Hospital Service Corporation ("MONOC") gained access to her Facebook account by having a supervisor summon a MONOC employee (who was one of Ms. Ehling's Facebook friends) into an office and coerce the employee into accessing his Facebook account in the supervisor's presence.[94] Ehling claimed that the supervisor viewed and copied her Facebook postings, one of which commented on a shooting that took place at the Holocaust Museum in Washington, DC.[95] Ehling asserted a claim for common law invasion of privacy.[96] The court held that "Plaintiff may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to protect her Facebook page from public viewing" and denied the motion to dismiss that claim.[97] The situation in *Ehling* is different from a situation where an employer asks a prospective employee or employee for his or her Facebook login and password to look at his or her Facebook profile. Instead, it involved a supervisor demanding access to and viewing

[92] *See* Gould, *supra* note 68; *see generally* Brian Wassom, *Common Law Invasion of Privacy Claims in Social Media*, WASSOM.COM (Jul. 2, 2013), http://www.wassom.com/common-law-invasion-of-privacy-claims-in-social-media-guest-post.html.
[93] Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F.Supp.2d 369, 373 (2012) (citing Bisbee v. John C. Conover Agency Inc., 186 N.J. Super. 335, 339 (App. Div. 1982)).
[94] *Ehling*, 872 F.Supp.2d at 370.
[95] *Id.*
[96] *Id.* at 372.
[97] *Id.* at 374. Notably, Ehling also alleged that defendants violated the New Jersey Wiretapping and Electronic Surveillance Control Act ("NJ Wiretap Act") "'by accessing without permission and improperly monitoring the electronic communications being stored on the plaintiffs Facebook account.'" *Id.* at 371–72. The court held that because the posting was in post-transmission storage when the defendants accessed it, the communication did not fall under the purview of the NJ Wiretap Act. *Id.* at 372.

one employee's Facebook account as a means to get access to another employee's account.[98] Still, an employee faced with the former situation could potentially bring a successful state claim for intrusion upon seclusion.

Nevertheless, in 2012, state lawmakers began introducing legislation to prevent employers from requesting passwords to employees' or prospective employees' personal social media accounts.[99] Notably, some states have enacted similar legislation to protect students at colleges and universities from having to grant school administrators access to their social networking accounts.[100] Employment-related legislation has been introduced or is pending in at least 36 states.[101] So far in 2013, ten states have enacted legislation, including Arkansas, Colorado, Illinois, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and Washington.[102] Parts IV and V will explore the positive and negative aspects of New Jersey's recently enacted law, compare New Jersey's law to some other state legislation, and propose a crucial way in which New Jersey's law could become more effective for employees.

IV. New Jersey's Legislation: "Compromising" Away Employee Protections?

A. The Christie Compromise

By March 2013, the first New Jersey legislation concerning employer social media password requests had passed both the Assembly and Senate.[103] This legislation's stated purpose was "prohibiting the requirement to disclose personal information for certain

[98] *Id.* at 370.
[99] *Employer Access to Social Media Usernames and Passwords 2013*, *supra* note 21.
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Bills 2012-2013*, NEW JERSEY LEGISLATURE – BILLS, http://www.njleg.state.nj.us/bills/BillView.asp (last visited Oct. 18, 2013).

electronic communications devices by employers."[104] Governor Christie, however, conditionally vetoed the proposed legislation in May 2013.[105] In his conditional veto, Christie stated, "In view of the over-breadth of this well-intentioned bill, I return it with my recommendations that more properly balance between protecting the privacy of employees and job candidates, while ensuring that employers may appropriately screen job candidates, manage their personnel, and protect their business assets and proprietary information."[106] Christie provided an example of "over-breadth" by noting that, under this bill, an employer interviewing a candidate for a marketing job would be prohibited from asking about the candidate's use of social networking so as to gauge the candidate's technological skills and media savvy.[107] According to Christie, "Such a relevant and innocuous inquiry would . . . subject an employer to protracted litigation, compensatory damages, and attorneys' fees – a result that could not have been the sponsors' intent."[108]

Christie recommended several substantive changes to the bill in his conditional veto.[109] First, he suggested eliminating the provision that prohibited employers from inquiring as to whether a current or prospective employee has an account or profile on a social networking website.[110] He notably recommended eliminating the section of the bill

[104] A.B. 2878, 215th Leg. (N.J. 2012), *available at* http://www.njleg.state.nj.us/2012/Bills/A3000/2878_I1.PDF.
[105] *Bills 2012-2013*, *supra* note 103; *see also* Brent Johnson, *Christie Signs Bill Banning N.J. Companies From Forcing Workers to Hand Over Social Media Passwords*, N.J.COM, Aug. 29, 2013, http://www.nj.com/politics/index.ssf/2013/08/christie_signs_bill_banning_nj_companies_from_forcing_workers_to_hand_over_social_media_passwords.html.
[106] A.B. 2878 (Third Reprint), at 2, *available at* http://www.njleg.state.nj.use/2012/Bills/A3000/2878_V2.PDF.
[107] *Id.* at 1.
[108] *Id.* at 1–2.
[109] *See id.* at 2–3; *see also* A.B. 2878 (Fourth Reprint), *available at* http://www.njleg.state.nj.us/2012/Bills/AL13/155_.PDF.
[110] A.B. 2878 (Third Reprint), at 2, *available at* http://www.njleg.state.nj.use/2012/Bills/A3000/2878_V2.PDF.

that provided for a private right of action.[111] Also, he suggested adding a section to permit employers to conduct an investigation "(1) for the purpose of ensuring compliance with applicable laws . . . or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on a personal account by an employee" and "(2) of an employee's actions based on the receipt of specific information about the unauthorized transfer of an employer's proprietary information[.]"[112] The Assembly and Senate accepted the governor's recommendations and passed the bill, which Governor Christie signed into law on August 28, 2013.[113] The act is set to take effect in December.[114]

B. Overview of New Jersey's Law as Enacted

New Jersey's law, as now enacted, starts with the premise that no employer[115] shall require or request a current or prospective employee to provide or disclose any username or password, or in any way provide the employer access to, a personal account through an electronic communications device.[116] Employers are prohibited from retaliating or discriminating against an individual because the individual has or was about to (1) refuse to provide or disclose any username or password; (2) report an alleged violation of the act to the Commissioner of Labor and Workforce Development; (3) testify, assist, or participate in any investigation, proceeding, or action concerning a violation of the act; or (4) otherwise oppose a violation of the act.[117]

---

[111] *Id.*
[112] *Id.*
[113] *Bills 2012-2013*, *supra* note 103.
[114] P.L.2013, c.155 (C.34:6B-5 et seq.) (approved Aug. 28, 2013), *available at* http://www.njleg.state.nj.us/2012/Bills/PL13/155_.PDF.
[115] An "employer" means an employer or employer's agent, representative, or designee. C.34:6B-5. However, the term "employer" does not include the Department of Corrections, State Parole Board, county corrections departments, or any State or local law enforcement agency. *Id.*
[116] C.34:6B-6.
[117] C.34:6B-8.

An employer who violates any provision of the act is subject to a civil penalty in an amount of $1,000 for the first violation and $2,500 for each subsequent violation.[118] The civil penalty is collectible by the Commissioner of Labor and Workforce Development.[119] As a result of Christie's legislative additions,[120] the act does not prevent an employer from implementing and enforcing a policy pertaining to the use of an *employer issued* electronic communications device or any accounts or services provided by the employer or that the employee uses for *business purposes*.[121] Moreover, as mentioned *supra*, the act does not prevent an employer from conducting an investigation "(1) for the purpose of ensuring compliance with applicable laws . . . or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on a personal account by an employee" or "(2) of an employee's actions based on the receipt of specific information about the unauthorized transfer of an employer's proprietary information, confidential information or financial data to a personal account by an employee."[122] Lastly, the act specifically states that it does not prevent an employer from viewing, accessing, or utilizing information about a current or prospective employee that can be obtained in the public domain.[123]

C. Comparison of New Jersey's Law to Other States

When compared to other states' legislation on this issue, New Jersey's legislation does provide some important employee protections. For example, New Jersey's law applies

[118] C.34:6B-9.
[119] *Id.*
[120] *See supra* note 109 and accompanying text.
[121] C.34:6B-10.
[122] *Id.*
[123] *Id.*

to both public and private employers.[124] While most states' laws do apply to both public and private employers,[125] California's existing law prohibits only private employers from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media.[126] Notably, there is a bill pending in California that would apply these provisions to public employers, but the bill is not enacted yet.[127]

New Jersey's law also seemingly addresses the problem of "shoulder surfing" while some other states' laws do not. Shoulder surfing is "the practice of demanding in, say, a job interview that someone log in to Facebook and reveal the privacy-protected parts of their profile."[128] New Jersey's law provides that "[n]o employer shall require or request a current or prospective employee to provide or disclose any user name or password, *or in any way provide the employer access to*, a personal account through an electronic communications device,"[129] which arguably includes the concept of shoulder surfing.[130] By contrast,

---

[124] C.34:6B-5. Again, the term "employer" does not include the Department of Corrections, State Parole Board, county corrections departments, or any State or local law enforcement agency. *Id.*

[125] *See Employer Access to Social Media Usernames and Passwords 2013, supra* note 21.

[126] A.B. 1844 (Cal. 2012), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201120120AB1844.

[127] *See* A.B. 25 (Cal. 2013), *available at* http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0001-0050/ab_25_bill_20121203_introduced.html; *Complete Bill History*, CALIFORNIA LEGISLATURE, http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=ab_25&sess=CUR&house=B&author=campos_%3Ccampos%3E (last visited Dec. 3, 2013).

[128] Martha C. White, *Facebook Weighs In and Blasts 'Shoulder Surfing' by Employers*, TIME, Mar. 23, 2012, http://business.time.com/2012/03/23/facebook-weighs-in-and-blasts-shoulder-surfing-by-employers/.

[129] C.34:6B-6 (emphasis added).

[130] States' laws that cover "shoulder surfing" include California, Michigan, Oregon, Washington, Illinois, and New Mexico. *See* A.B. 1844 (Cal. 2012), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201120120AB1844; H.B. 5523, 96th Leg., 2012 Reg. Sess. (Mich. 2012), *available at* http://www.legislature.mi.gov/documents/2011-2012/publicact/pdf/2012-PA-0478.pdf; H.B. 2654, 77th Leg. Assemb., 2013 Reg. Sess. (Or. 2013), *available at* https://olis.leg.state.or.us/liz/2013R1/Measures/Text/HB2654/Enrolled; S.B. 5211, 63rd Leg., 2013 Reg. Sess. (Wash. 2013), *available at* http://apps.leg.wa.gov/documents/billdocs/2013-

Maryland's law does not include language to implicate "shoulder surfing," stating instead that "an 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."[131] Utah's law also does not prohibit "shoulder surfing" on its face.[132]

Furthermore, New Jersey's current law does not provide a private right of action but it does provide an administrative remedy.[133] New Jersey's law states that an employer who violates any provision of the act shall be subject to a civil penalty in an amount not to exceed $1,000 for the first violation and $2,500 for each subsequent violation.[134] The civil penalty is collectible by the Commissioner of Labor and Workforce Development in a summary proceeding.[135] Meanwhile, the laws enacted in Arkansas, Illinois, and New Mexico do not provide either a private right of action *or* an administrative remedy.[136]

Finally, many of the states that have enacted these social media laws have included clauses permitting employers to investigate employee misconduct on certain conditions.[137] New Jersey's law provides that nothing in the act shall prevent an employer from conducting an investigation "(1) for the purpose of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related misconduct based on the

---

14/Pdf/Bills/Senate%20Passed%20Legislature/5211-S.PL.pdf; S.B. 2306, 98th Gen. Assemb. (Ill. 2013), *available at* http://www.ilga.gov/legislation/98/SB/PDF/09800SB2306lv.pdf; S.B. 371, 2013 Reg. Sess. (N.M. 2013), *available at* http://www.nmlegis.gov/Sessions/13%20Regular/final/SB0371.pdf.

[131] S.B. 433 (Md. 2012), *available at* http://legiscan.com/MD/text/SB433/id/642509.

[132] H.B. 100, 2013 Gen. Sess. (Utah 2013), *available at* http://le.utah.gov/~2013/bills/hbillenr/HB0100.pdf.

[133] C.34:6B-9.

[134] *Id.*

[135] *Id.*

[136] *See* H.B. 1901, 89th Gen. Assemb., Reg. Sess. (Ark. 2013), *available at* http://www.arkleg.state.ar.us/assembly/2013/2013R/Bills/HB1901.pdf; S.B. 2306, 98th Gen. Assemb. (Ill. 2013), *available at* http://www.ilga.gov/legislation/98/SB/PDF/09800SB2306lv.pdf; S.B. 371, 2013 Reg. Sess. (N.M. 2013), *available at* http://www.nmlegis.gov/Sessions/13%20Regular/final/SB0371.pdf.

[137] *See Employer Access to Social Media Usernames and Passwords 2013*, *supra* note 21.

receipt of *specific information* about activity on a personal account by an employee[.]"[138] California's law, by contrast, provides that nothing in the act shall affect "an employer's existing rights and obligations to request an employee to divulge personal social media *reasonably believed* to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding."[139] Though the states' standards are similar, it is possible that New Jersey's law provides slightly greater employee protections from potentially intrusive investigation based on its requirement for "specific information."

V. The Need for a Private Right of Action

While there are some employee protections that the New Jersey legislation provides that other states do not, New Jersey's law will likely still fail to provide adequate employee protections because it lacks a private right of action. Despite Governor Christie's elimination of a private right of action in New Jersey's law,[140] the law should be revised to include a private right of action with limitations.

A. Private Right of Action in Other Laws

Currently, there are several employment-related federal statutes that provide employees a private right of action.[141] The Family Medical Leave Act ("FMLA"),[142] the Age Discrimination in Employment Act ("ADEA"),[143] and Title VII of the Civil Rights Act

[138] C.34:6B-10.
[139] A.B. 1844 (Cal. 2012), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201120120AB1844.
[140] *See supra* note 111.
[141] *See infra* notes 142–144.
[142] *See* 29 U.S.C. § 2617(a)(2) (2008).
[143] *See* 29 U.S.C. § 626(c)(1) (2013).

of 1964,[144] among others, all allow individuals to enforce their provisions through a private right of action. There are also New Jersey state employment-related laws that provide employees a private right of action. New Jersey's Law Against Discrimination ("NJLAD")[145] and the New Jersey Family Leave Act ("FLA")[146] each specifically provide employees a private right of action.

Of particular importance, however, is the fact that several other states that have enacted specific social media password legislation have provided employees a private right of action within those laws.[147] For example, Colorado's law, signed by the governor on May 11, 2013, provides that an aggrieved applicant or employee may institute a civil action for a violation of the act in a court of competent jurisdiction within one year after the date of the alleged violation.[148] In response, the court may award the aggrieved person "(a) injunctive relief; (b) compensatory and consequential damages incurred by the person as a result of the violation; and (c) reasonable attorney fees and court costs."[149] Michigan's law, signed by the governor on December 27, 2012, also provides a private right of action.[150] This private right of action states, among other things, that "[a]n individual who is the subject of a violation of [the] act may bring a civil action to enjoin a violation [ ] and may

[144] *See* 42 U.S.C. § 2000e-5(f)(1) (2013).
[145] *See* N.J.S.A. § 10:5-13 (2013).
[146] *See* N.J.S.A. 34:11B-11 (2013).
[147] *See infra* notes 148, 150, 152, 155.
[148] H.B. 1046, 69th Gen. Assemb., First Reg. Sess. (Colo. 2013), *available at* http://www.leg.state.co.us/CLICS/CLICS2013A/csl.nsf/fsbillcont3/B1355B3A769E5C4A87257A8E0073C3BA?Open&file=1046_01.pdf.
[149] *Id.*
[150] H.B. 5523, 96th Leg., 2012 Reg. Sess. (Mich. 2012), *available at* http://www.legislature.mi.gov/documents/2011-2012/publicact/pdf/2012-PA-0478.pdf.

recover not more than $1,000.00 in damages plus reasonable attorney fees and court costs."[151]

Utah's law, signed by the governor on March 26, 2013, similarly provides a private right of action.[152] According to Utah's law, a person aggrieved by a violation of the act may bring a civil cause of action against an employer in a court of competent jurisdiction.[153] The law states that if the court finds a violation, "the court shall award the aggrieved person not more than $500."[154] Additionally, Washington's law, signed by the governor on May 21, 2013, also provides a private right of action.[155] Washington's law provides that an employee or applicant aggrieved by a violation of the act may bring a civil action in a court of competent jurisdiction.[156] The court may do the following:

> (1) Award a prevailing employee or applicant injunctive or other equitable relief, actual damages, a penalty in the amount of five hundred dollars, and reasonable attorneys' fees and costs; and
> (2) [A]ward any prevailing party against whom an action has been brought for a violation of section 1 of [the] act reasonable expenses and attorneys' fees upon final judgment and written findings by the trial judge that the action was frivolous and advanced without reasonable cause.[157]

In addition to these states that have enacted social media laws providing a private right of action, there are other states with social media bills pending that include a private right of action in the proposed bill.[158]

---

[151] *Id.*
[152] H.B. 100, 2013 Gen. Sess. (Utah 2013), *available at* http://le.utah.gov/~2013/bills/hbillenr/HB0100.pdf.
[153] *Id.* at § 34-48-301.
[154] *Id.*
[155] S.B. 5211, 63rd Leg., 2013 Reg. Sess. (Wash. 2013), *available at* http://apps.leg.wa.gov/documents/billdocs/2013-14/Pdf/Bills/Senate%20Passed%20Legislature/5211-S.PL.pdf.
[156] *Id.* at Sec. 2.
[157] *Id.*
[158] *See* H.B. 149 (Ga. 2013), *available at* http://www.legis.ga.gov/Legislation/20132014/129229.pdf; H.P. 838, 126th Leg. (Me. 2013), *available at* http://www.mainelegislature.org/legis/bills/bills_126th/billtexts/HP083801.asp; L.B. 58, 103rd Leg., 1st Sess.

B. The Importance of Private Rights of Action in Employment Legislation

Private rights of action are important in both federal and state employment legislation. Scholars have noted how laws' promises gain "'teeth'" in the form of a private right of action.[159] Moreover, private rights of action give employees "meaningful choices about which remedies to pursue."[160] More specifically, private enforcement regimes can "take advantage of private information to detect violations; . . . [and] emit a clear and consistent signal that violations will be prosecuted, providing insurance against the risk that a system of administrative implementation will be subverted[.]"[161] Private enforcement regimes "limit the need for direct and visible intervention by the bureaucracy . . . [and] facilitate participatory and democratic governance."[162]

A private right of action in New Jersey's social media law would give employees and prospective employees a viable way to vindicate their rights and the remedial purposes of New Jersey's law. Currently, the law includes in its "penalties" section only that an employer who violates any provision of the act is subject to a civil penalty in an amount not to exceed $1,000 for the first violation and $2,500 for each subsequent violation, collectible by the Commissioner of Labor and Workforce Development.[163] Thus, employees and prospective employees remain dependent on the Commissioner of Labor and Workforce Development for enforcement of the law and receive no monetary award themselves.[164] A private right of action would not only be helpful to employees, but also likely cause

(Neb. 2013), *available at* http://nebraskalegislature.gov/FloorDocs/Current/PDF/Intro/LB58.pdf; S.B. 493 (R.I. 2013), *available at* http://webserver.rilin.state.ri.us/BillText13/SenateText13/S0493.htm.

[159] Deborah Thompson Eisenberg, *Opening the Doors to the Local Courthouse: Maryland's New Private Right of Action for Employment Discrimination*, 9 U. MD. L.J. RACE, RELIGION, GENDER & CLASS 7, 8 (2009).

[160] *Id.* at 10.

[161] Stephen B. Burbank et al., *Private Enforcement*, 17 LEWIS & CLARK L. REV. 637, 662 (2013).

[162] *Id.*

[163] C.34:6B-9.

[164] *See generally id.*

employers to take the law more seriously.[165] A private right of action would show that these types of claims will not get lost in any sort of administrative shuffle or, for that matter, become subject to administrative inaction.[166]

C. A Proposed Standard for a Private Right of Action

Given the practical significance of private rights of action in employment laws, and also the feasibility of including a private right of action in social media legislation,[167] New Jersey should amend its law to include a private right of action. Governor Christie previously eliminated the private right of action from Assembly Bill 2878.[168] Nevertheless, there are ways that a limited private right of action could be included in the law to provide greater employee protections and maintain Governor Christie's sought-after "balance."[169]

One way in which New Jersey could place limitations upon its private right of action is to cap the amount of recovery that an employee can receive from a suit. Washington's law effectively does this[170] and is a realistic example upon which New Jersey should base its private right of action. Washington's law provides that a court may award a prevailing employee or applicant injunctive or other equitable relief, actual damages, a penalty in the amount of five hundred dollars, and reasonable attorneys' fees and costs.[171] This approach is sensible for several reasons. First, the law offers the possibility of injunctive relief but does not limit its remedy to injunctive relief.[172] The opportunity for more than injunctive

[165] *See generally* Eisenberg, *supra* note 159, at 7.
[166] *See* Burbank et al., *supra* note 161, at 662.
[167] *See supra* notes 147–157 and accompanying text.
[168] *See supra* note 111.
[169] *Id.*
[170] S.B. 5211, 63rd Leg., 2013 Reg. Sess. (Wash. 2013), *available at* http://apps.leg.wa.gov/documents/billdocs/2013-14/Pdf/Bills/Senate%20Passed%20Legislature/5211-S.PL.pdf.
[171] *Id.* at Sec. 2.
[172] *Id.*

relief makes it more likely that an employee and an employee-side attorney will actually be interested in bringing the suit. Next, the law provides the possibility of actual damages.[173] While these may be more difficult to show for a prospective employee, it certainly may be possible for a current employee to prove lost wages or even termination in relation to his or her provision or refusal to provide a social media username and password.[174] Washington's law also provides a penalty in the amount of $500.[175] This capped penalty provides another, albeit somewhat minor, incentive for employees to bring suit, but at the same time it is more amenable to employers than a broad allowance for punitive damages would be.[176] Finally, the law provides reasonable attorneys' fees and costs,[177] another incentive for employees and attorneys to bring the suit in the first place. All together, Washington's law provides several specific and reasonable remedies for aggrieved employees and prospective employees. New Jersey could greatly improve the employee protections of its law if it adopts a private right of action like the one in Washington's law.

Furthermore, New Jersey's law would benefit and likely pass muster under Governor Christie's scrutiny if it added a second clause to its private right of action similar to the one included in Washington's law. Washington's law also provides that a court may award any prevailing party against whom an action has been brought for a violation of section 1 of the act reasonable expenses and attorneys' fees upon final judgment and written findings by the

---

[173] *Id.*
[174] *See generally* Del Riego et al., *supra* note 29, at 21.
[175] S.B. 5211 at Sec. 2.
[176] Rhode Island's proposed law, for example, broadly provides that the court may "award to a prevailing applicant, employee or student punitive damages in addition to any award of actual damages, and reasonable attorneys' fees and costs[.]" S.B. 493 (R.I. 2013), *available at* http://webserver.rilin.state.ri.us/BillText13/SenateText13/S0493.htm.
[177] S.B. 5211 at Sec 2.

trial judge that the action was frivolous and advanced without reasonable cause.[178] A clause like this in New Jersey's private right of action would not only serve to prevent employees from bringing meritless actions, but also provide more "balance" and fairness for employers.[179] Governor Christie previously recommended removing the private right of action from New Jersey's law, noting that there needed to be a more proper "balance between protecting the privacy of employees and job candidates, while ensuring that employers may appropriately screen job candidates, manage their personnel, and protect their business assets and proprietary information."[180] Adding a private right of action back into New Jersey's law will do nothing to take away employers' ability to screen job candidates, manage their personnel, and protect their business assets and proprietary information. Moreover, the addition of this second clause will ensure that so long as employers abide by the law and act in "good faith,"[181] they will not have to worry about the costs associated with defending potential frivolous employee actions against them.

D. A Proposed Draft of a Private Right of Action

With Washington's law serving as a template,[182] New Jersey could easily reincorporate a private right of action into its social media legislation. Based on the considerations in Part V.C *supra*, the private right of action should include the possibility

[178] *Id.*
[179] A.B. 2878 (Third Reprint), at 2, *available at* http://www.njleg.state.nj.use/2012/Bills/A3000/2878_V2.PDF.
[180] *Id.*
[181] Notably, in his conditional veto, Governor Christie seems particularly concerned about "good faith" employers being subjected to lawsuits. *See id.* For example, in suggesting the elimination of a section of the proposed bill that would disallow an employer from asking whether a job candidate has a personal social media account, Christie said, "Such a relevant and innocuous inquiry would, under this bill, subject an employer to protracted litigation, compensatory damages, and attorneys' fees – a result that could not have been the sponsors' intent." *Id.* at 1. By including a provision in the bill's private right of action stating that a prevailing employer may be awarded reasonable expenses and attorneys' fees upon a finding that an action is frivolous, however, "good faith" employers will ultimately still find protection.
[182] *See* S.B. 5211, 63rd Leg., 2013 Reg. Sess. (Wash. 2013), *available at* http://apps.leg.wa.gov/documents/billdocs/2013-14/Pdf/Bills/Senate%20Passed%20Legislature/5211-S.PL.pdf.

for employees or prospective employees to be awarded injunctive relief, compensatory damages, a capped penalty, and reasonable attorneys' fees and costs.[183] The private right of action should also include a provision stating that a prevailing employer may be awarded reasonable expenses and attorneys' fees upon a finding that an action is frivolous.[184] Notably, New Jersey's previously proposed private right of action, which was vetoed by Governor Christie, did include some of these aspects.[185] In order to both appease Christie's concerns and provide greater protection to employees, New Jersey's social media law should be revised to include a private right of action drafted as follows:

> Upon violation of any provision of this act, an aggrieved person may, in addition to any other available remedy, institute a civil action in a court of competent jurisdiction, within one year from the date of the alleged violation. In response to the action, the court may:
>
> (1) Award a prevailing employee or applicant (1) injunctive or other equitable relief; (2) compensatory damages, including compensation for lost wages; (3) a penalty in the amount of no more than five hundred dollars; and (4) reasonable attorneys' fees and costs; and
> (2) Award any prevailing employer against whom an action has been brought for violation of this act reasonable expenses and attorneys' fees upon final judgment and written findings by the trial judge that the action was frivolous and advanced without reasonable cause.

The introductory clause of this draft is modeled after New Jersey's previous private right of action, which Governor Christie rejected in its totality.[186] This introductory language is important to include in the private right of action, however, particularly because it limits the time frame in which a civil action may be brought. By providing that a civil action must be brought "within one year from the date of the alleged violation,"[187] the clause

[183] *See supra* Part V.C.
[184] *Id.*
[185] A.B. 2878 (Fourth Reprint), at 2–3, *available at* http://www.njleg.state.nj.us/2012/Bills/AL13/155_.PDF.
[186] *Id.*
[187] *Id.*

ensures that employers will not have to potentially defend against old claims. Sections (1) and (2) of this draft are modeled after Washington's law,[188] with a few minor changes. For example, this proposed draft includes an example of compensatory damages (i.e., lost wages), while Washington's law does not.[189] Though "lost wages" are only one example of compensatory damages, the explicit mention of them gives employees an idea of what compensatory damages may mean. Additionally, this draft includes the phrase "no more than" five hundred dollars with regard to the penalty and Washington's private right of action does not.[190] This phrase provides clarification that the penalty is capped and is not to exceed five hundred dollars. Finally, this draft changes the language of Section (2) to state "[a]ward any prevailing employer" as opposed to "[a]ward any prevailing party," as stated in Washington's law,[191] in order to further emphasize that Section (2) provides protections for employers. In sum, New Jersey's incorporation of this draft into its current social media legislation would be an effective way to provide employees and job candidates with greater protection under the law and, at the same time, to maintain certain safeguards for employers.[192]

E. Providing a Private Right of Action Will Counter Other Legislative Shortcomings

[188] *See* S.B. 5211, 63rd Leg., 2013 Reg. Sess. (Wash. 2013), *available at* http://apps.leg.wa.gov/documents/billdocs/2013-14/Pdf/Bills/Senate%20Passed%20Legislature/5211-S.PL.pdf.
[189] *Id.*
[190] *Id.*
[191] *Id.*
[192] Although jurisdictional issues are beyond the scope of this Comment, it is worthwhile to note that New Jersey's legislation likely should specify jurisdictional limitations in relation to its private right of action. For example, the law may be amended to state that the private right of action is limited to those who are current employees within the state of New Jersey and those who have applied to work within the state of New Jersey. Should New Jersey choose to reincorporate a private right of action into its law, further analysis and consideration will be necessary in this area.

New Jersey's inclusion of this proposed private right of action would also likely go a long way in easing other potential employee-side complaints about the current law. Aside from the current lack of a private right of action, there are other aspects of the law that will foreseeably receive criticism from employees or their proponents. For instance, New Jersey's law excludes law enforcement agents from its definition of "employer," and, therefore, excludes them from coverage under the act.[193] While this may seem sensible under certain conditions,[194] many states' social media laws, as enacted, do not include such an exception.[195] Also, employee-side proponents are likely to take issue with the section added to New Jersey's law, based entirely on Governor Christie's recommendation, which allows employers to conduct an investigation into work-related employee misconduct based on the receipt of "specific information about activity on a personal account by an employee."[196] Employees may argue that even though this section calls for "specific information," that standard can easily be abused. Though these concerns are likely to persist, the addition of this proposed private right of action to New Jersey's law will certainly help in the efforts to placate employees and their advocates.

Conclusion

In recent years, reports have surfaced of employers asking for employees' or prospective employees' social media logins and passwords, most typically to access their Facebook accounts.[197] While some employers have advanced justifications for the

[193] *See* C.34:6B-5 (The term "employer" does not include the Department of Corrections, State Parole Board, county corrections departments, or any State or local law enforcement agency.).
[194] *See* Sullivan, *supra* note 9 ("It's easy to see why an agency that hires prison guards would want to sneak a peek at potential employees' private online lives. [P]risons are trying to avoid hiring guards with potential gang ties[.]")
[195] *See Employer Access to Social Media Usernames and Passwords 2013*, *supra* note 21.
[196] C.34:6B-10.
[197] *See supra* Part I.

practice,[198] employees and their proponents have voiced concern that this practice is an unacceptable encroachment on employee privacy.[199] Facebook itself has asserted that employers should not ask prospective employees or employees to provide their passwords and that doing so violates Facebook's Statement of Rights and Responsibilities.[200] Still, it has remained unclear what exact protections prospective employees or employees have in this situation.

The Stored Communications Act ("SCA") and the Computer Fraud and Abuse Act ("CFAA"), though powerful federal laws, may or may not reach situations where employers ask for employees' or prospective employees' passwords to access their personal accounts.[201] There has been an influx of legislative attempts to pass federal laws that would specifically address employers' social media password requests.[202] These laws have failed, however, to gain the requisite political support.[203] Most notably, some states have implemented laws that provide protections for employees in the context of social media password requests.[204] On August 28, 2013, New Jersey signed into law its own legislation to this effect.[205]

In comparison to some other states' laws enacted in this area, New Jersey's law seemingly keeps pace. Nevertheless, in order to create true employer-employee balance and provide meaningful remedies for aggrieved employees, New Jersey's law should reincorporate the private right of action that it intentionally left out. Washington's law

[198] *See supra* Part II.
[199] *Id.*
[200] *Id.*
[201] *See supra* Part III.A.
[202] *See supra* Part III.B.
[203] *Id.*
[204] *See supra* Part III.C.
[205] *Id.*

provides an excellent example of a realistic and workable private right of action. New Jersey should model its private right of action after Washington's to provide aggrieved employees greater recourse and, at the same time, maintain certain remedial limitations for the sake of employers.