5-1-2013

Stop in the Name of Privacy: Legislators Atwitter Over Social Media Password Rights

Michael Joseph Mouridy

STOP IN THE NAME OF PRIVACY:
Legislators Atwitter over Social Media Password Rights

Michael Mouridy

Introduction

Imagine you are a Human Resources recruiting director for Buzzfeed.com. Buzzfeed is a self-proclaimed "new kind of Media Company" that seeks to deliver high-quality original reporting, insight, and viral content across a wide array of subject areas. A position has opened up for a "Blogger" that you need to fill immediately. Currently, to become a "Blogger" for Buzzfeed you must meet the following requirements: high emotional intelligence, the ability to take perspective of others, a positive, curious, playful disposition (no haters), a competitive drive, genuine, wide-eyed love of pop culture in all its forms, a proven ability to get viral traffic, and an established social media presence.[1] The initial requirements such as an applicant's disposition, emotional intelligence, and competitive drive can be determined from the typical interview process of an in person interview, asking for references, and making a judgment call. However, these characteristics might be more easily determined by a Facebook search of the applicant to see their recent and past posts to gain a general feel for the applicant. Also, it would be incredibly helpful to look at the applicant's social media accounts when determining if the applicant has an established social media presence. So why not demand to view the candidates social media account as part of the application process?

---

[1] BUZZFEED.COM, http://www.jobscore.com/jobs/buzzfeed/blogger/c6uPFgcyKr4OEDeJe4efaV?ref=rss&sid=68 (last visited Dec. 5, 2012).

In early 2012, it became widely publicized that several employers were asking job candidates for their passwords to social networking sites, such as Facebook, Twitter, and LinkedIn. Many of these employers were demanding this information as part of the interview process. Providing one's password obviously affords access to information, photos, and data that was often not shared with anyone outside of that candidate's private network. In most of these cases, a candidate was not considered for employment or feared that they would not be considered for employment if they refused to turn over their passwords.

This paper will first provide more background into the prevalence of employers using social media to research job applicants and the ways in which employers are performing this research. The paper will then delve into the response from state and federal legislators to these new employer practices. Lastly, the paper will provide a general overview of the current laws already in place that might disincentivize employers from using social media in this fashion.

The Newly Popular Social Media "Background checks"

Social media has grown exponentially in the past decade. Apart from the grown of individual users, there has been a growth of employers using social media to not only further enhance their companies marketing and sales, but also to determine their new hires. In a 2009 survey conducted by CareerBuilder.com, 45 percent of companies use social media sites to screen potential hires, with most of them looking at Facebook (29 percent) and LinkedIn (26 percent).[2] In the same study, of more than 2,600 hiring managers surveyed, 35 percent had

[2] Nicolas Jackson, *Infographic: How Employers Use Social Media to Hire and Fire*, THEATLANTIC, (August 15, 2011), http://www.theatlantic.com/technology/archive/2011/08/infographic-how-employers-use-social-media-to-hire-and-fire/243599/.

rejected candidates after finding objectionable material, including photos of them using drugs, bad-mouthing previous employers and lying about their qualifications.[3]

One troubling aspect of this new type of background check is that potential employees will likely not be afforded an opportunity to provide an explanation as to the information employers see on social media. For example, according to the Society for Human Resource Management, 73 percent of companies surveyed said they do not give the applicants a chance "to explain questionable information."[4] A further danger to the applicant is the chance that the employer may actually be investigating the wrong social media account of someone with the same name as the applicant.[5] Of course, an employer's investigation of an applicants social media account could also result in the applicant getting hired. In the previously mentioned 2009 Careerbuilder.com study, three in ten hiring managers (29 percent) said they have found something that has caused them to hire a candidate such as getting a "good feel" for the applicant or that the applicant conveyed a good personal image. [6]

However, this seemingly rampant practice of using social media to screen applicants may stem from the fact that employers have a duty to prevent negligent hiring. The tort of negligent hiring is based on the principle that a person conducting an activity through employees is subject to liability for harm resulting from conduct in the employment of improper persons involving risk of harm to others.[7] Almost all jurisdictions recognize this tort and liability is predicated on the employer's hiring of a person when the employer knew or should have reasonable known that

---

[3] Steve Johnson, *Those party photos could cost you a job*, CHI. TRIB. (Jan. 17, 2012), http://www.chicagotribune.com/features/tribu/ct-tribu-facebook-job-dangers-20120117,0,1257938.column.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Connes v. Molalla Transport System, Inc., 831 P.2d 1316 (Colo. 1992).

the person, by reason of some attribute of character or prior conduct, would create an undue risk of harm to others in carrying out his or her employment responsibilities.[8] Thus, employers in order to protect themselves from future liability might be incentivized to do a Facebook search of the applicant, which most likely will require asking for their applicant's password. While this might protect employers from the tort of negligent hiring, it will open a pandora box of other legal risks for the employer.

State and Federal Statutes

In response to the widely published cases involving an employer demanding a job applicant's social media password, both the state and federal legislature have stepped in. Currently, there are two federal bills attempting to remedy this issue that have been introduced to Congress. In addition, fourteen states have introduced legislation in 2012 addressing this issue and a couple of states already signed the bills into law.[9] As evidenced from the discussion below, all of the statutes have the basic goal of preventing employers from demanding applicants or current employees from handing over their log-in information for social media sites like Facebook. However, each statute is very different in its scope, enforcement, and remedies.

Federal Statutes

As previously mentioned, there has been recent Congressional action regarding bills that would prohibit employers from asking employees and job applicants for their social media passwords. Representative Ed Perlmutter of Colorado first proposed a bill that would have added

[8] *Id.* at 1321.
[9] Pam, Greenberg, *Employer Access to Social Media Usernames and Passwords*, NCSL.ORG, (Nov. 16, 2012), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.

an amendment to the Federal Communications Process Reform Act of 2012.[10] The amendment was ultimately voted down by the House of Representatives, 236 to 184, but contained the following language:

> Nothing in this Act or any amendment made by this Act shall be construed to limit or restrict the ability of the Federal Communications Commission to adopt a rule or to amend an existing rule to protect online privacy, including requirements in such rule that prohibit licensees or regulated entities from mandating that job applicants or employees disclose confidential passwords to social networking websites.[11]

The amendment was essentially a party-line vote with the Republicans voting the bill down. However, the amendment has been understood to not stand for Republican's opposition to password protection, but rather as a transparent delay tactic by representative Perlmutter.[12] As one critic indicates, "if Perlmutter actually wanted to add that pro-privacy section to the bill, he could have suggested an amendment instead of returning to the committee."[13]

Shorty after the House of Representatives voted down the above legislation, new legislation was introduced regarding password protection, and this time it specifically addressed the issue of job applicants being asked for their social media passwords. The Social Networking Online Protection Act ("SNOPA") was introduced in the House of Representatives on April 27, 2012.[14] SNOPA prohibits an employer from asking its employees and applicants for Facebook and other social media passwords. The bill also prohibits schools from asking its students or

---

[10] Sarah Jacobsson Purewal, *Facebook Password Amendment Rejected by Congress*, PCWORLD, (March 29, 2012), http://www.pcworld.com/article/252837/facebook_password_amendment_rejected_by_congress.html.
[11] *Id*.
[12] Declan McCullah, *House votes down plan to block employers from Facebook snooping*, (March 28, 2012), http://news.cnet.com/8301-31921_3-57406124-281/house-votes-down-plan-to-block-employers-from-facebook-snooping.
[13] *Id*.
[14] Allen Smith, *Social Networking Online Protection Act Introduced*, SHRM.ORG, (May 1, 2012), http://www.shrm.org/LegalIssues/FederalResources/Pages/SNOPA.aspx.

potential students for their social media passwords. Specifically, it provides that it would be unlawful for any employer to: require or request any employee or applicant for employment to provide their user name, password, or other means for accessing a private email account or social networking website account; or discharge, discipline, or discriminate against any employee or applicant because of the employee's refusal to provide such information or because the employee or applicant filed a complaint or testified in a proceeding related to SNOPA.[15]

SNOPA includes a civil penalty provision up to $10,000 and gives the Secretary of Labor the authority to bring an action for injunctive relief. Unlike employment discrimination statutes that typically do not apply to very small businesses, SNOPA would apply to all employers, regardless of workforce size, as it expressly defined the term "employer" as meaning "any person acting directly or indirectly in the interest of an employer in relation to an employee or an applicant for employment."[16]

Another proposed bill, the Password Protection Act of 2012 ("PPA"), was introduced in both houses of Congress on May 9, 2012.[17] The PPA would amend the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, by adding the following provision among its prohibitions:

> [F]or the purposes of employing, promoting, or terminating employment, compel[ling] or coerc[ing] any person to authorize access, such as by providing a password or similar information through which a computer may be accessed, to a protected computer that is not the employer's protected computer, and thereby obtains information from such protected computer.[18]

---

[15] Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2nd Sess. 2012).

[16] *Id.*

[17] Lance Whitney, *Democrats to employers: Stop asking for Facebook passwords*, (May10, 2012). http://www.cbsnews.com/8301-501465_162-57431867-501465/democrats-to-employers-stop-asking-for-facebook-passwords.

[18] Password Protection Act of 2012, H.R. 5684, 112th Cong. (2nd Sess. 2012).

The PPA prohibits employers from forcing perspective or current employees from providing access to their own private personal data systems as a condition of employment. However, the bill still retains employers' rights to govern access to social networking sites within office hours and set policies for employer-operated computer system accounts.

The PPA would also prohibit employers from disciplining or discriminating against any person who fails to provide the employer with access to the employee's protected computer.[19] The PPA carves out exemptions for the military and federal agencies, such as the National Security Agency and Defense Intelligence Agency, which deal with classified information. Also, the PPA adopts the same definition of employer as found in the Genetic Information Nondiscrimination Act of 2008, which would make it applicable to most businesses with 15 or more employees.[20]

The PPA's language makes the bill very broad in scope. As written, the PPA would not just apply to social networks like Facebook or LinkedIn, but would also apply when an employer compels an employee into providing access to information held on any computer that isn't owned or controlled by the employer.[21] This language would have the PPA apply to personal email accounts and smart phones, including iPhones. The drafters intended to make this bill adaptable and tried to craft language that would be sufficiently flexible to remain relevant as new technologies are developed.[22] However one criticism of the PPA is that, unlike SNOPA, it does not provide protection to students and universities.[23]

---

[19] *Id.*
[20] *Id.*
[21] Chris Calabrese, *Password Protection Act of 2012: A Good Start Against Employer Snooping*, ACLU.ORG, (May, 9, 2012). http://www.aclu.org/blog/technology-and-liberty/password-protection-act-2012-good-start-against-employer-snooping.
[22] *Id.*
[23] *Id.*

State Legislation

Maryland

Maryland became the first state to legislate against employers requiring job applicants and employees to disclose their social media passwords. On May 2, 2012, Maryland Governor Martin O'Malley signed into law a bill that protects employees and applicants against mandatory disclosure of social media passwords and other personal account information.[24]

The law took effect on October 1, 2012, and states 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."[25] The bill is considered to have a broad scope and effectively bars any request of an employer for access to the personal accounts of either an applicant or an employee.[26] The bill also prohibits employers from discharging, disciplining, or penalizing an employee for an employee's refusal to disclose such account information.[27] Similarly, an employer cannot reject an applicant for refusing to disclose social media account log-in credentials.

The Maryland law includes a set of very narrow exceptions. These exceptions allow for an employer to gain access to the employee's password when it receives a report about violations regarding the employee violating securities and financial law or regarding unauthorized downloading of the employer's proprietary information or financial data.[28] Also, the law only protects an employee's "personal" accounts, so if an employee were to establish a Twitter

[24] Catherine Cho, *Maryland becomes first state to prohibit employers from asking for Facebook logins*, WASH. POST, (May 3, 2012), http://www.washingtonpost.com/blogs/capital-business/post/maryland-becomes-first-state-to-prohibit-employers-from-asking-for-facebook-logins/2012/05/03/gIQAsE1GzT_blog.html.
[25] *Md*. Lab. & Empl. Code § 3-712.
[26] 22 No. 8 Md. Emp. L. Letter 1.
[27] *Id.*
[28] *Id.*

account for official business purposes, the employer could require that the employee provide the log- in credentials.[29] However, it is likely that determining whether an account is entirely personal or entirely business related is a tricky issue that courts going to have to deal with.

A noteworthy aspect of the Maryland law is that it does not contain an enforcement provision nor does it contain remedies or penalties provisions.[30] Therefore an employee who is discharged for failure to disclose a social media password might be able to argue wrongful discharge in violation of public policy. However, it is unclear whether an employee who is disciplined but not terminated would have a claim.

The bill signing comes just over a year after the Maryland Department of Public Safety and Correctional Services ("MDPSCS") suspended its own practice of asking officers to provide login information for Facebook or other social media websites they may have used. This former practice was the center of a highly publicized case. The case involved a former corrections officer at the MDPSCS, Robert Collins, who challenged the MDPSCS's demand that he provide them with access to his private Facebook account.[31] Collins was looking to be reinstated with the MDPSCS in 2010 when he was asked for his Facebook password on the job interview. Collins provided his password because he "really need[ed] [his] job."[32] The interviewer then logged into Collin's Facebook account and searched through his messages, wall posts, and pictures.[33]

---

[29] 19 No. 6 Kan. Emp. L. Letter 1.
[30] Philip L. Gordon, *Maryland "Facebook Law" Raises New Obstacles For Employers Vetting Applicants And Investigating Employees, But With Important Exceptions*, (April 11, 2012), http://privacyblog.littler.com/2012/04/articles/social-networking-1/maryland-facebook-law-raises-new-obstacles-for-employers-vetting-applicants-and-investigating-employees-but-with-important-exceptions/.
[31] Doug Gross, *ACLU: Facebook password isn't your boss' business*, CNN.COM, (March 22, 2012), http://www.cnn.com/2012/03/22/tech/social-media/facebook-password-employers/index.html.
[32] *Id.*
[33] *Id.*

MDPSCS attempted to justify its actions by explaining that it needed to check the Facebook pages of its corrections officers in order to ensure that they were not engaging in any gang-related activity.[34] Mr. Collins contacted the American Civil Liberties Union ("ACLU") to represent him.

The ACLU alleged that the MDPSCS's conduct violated Section 2701 of the Stored Communications Act, the First and 14th amendments of the U.S. Constitution and constituted an invasion of Mr. Collins's privacy. Shortly thereafter, the MDPSCS agreed to cease demanding access to social media accounts. While ACLU believed that it had a variety of grounds upon which to challenge the MDPSCS's practices, Maryland did not have a specific law that clearly addressed this issue. Hence, the legislation passed in May was a direct result of Maryland attempting to make sure a case like Collins' never happened again.

Illinois

Illinois is the second state to pass legislation that prevents employers from requesting employees or prospective employees social media passwords by passing an amendment to their already existing Right to Privacy in the Workplace Act. The new law makes it unlawful for an employer to "request or require any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website" or "demand access in any manner to an employee's or prospective employee's account or profile on a social networking website."[35]

The statute defines a "social networking website" to mean an Internet-based service that allows individuals to construct a public or semi-public profile within a bounded system, to create a list of other users with whom they share a connection within the system, and to view and

[34] *Id.*
[35] 820 Ill. Comp. Stat. 55/10.

navigate their list of connections and those made by others, but does not include electronic mail. This statute would seem to cover most of the currently popular social networking sites, such as Facebook, MySpace, and Twitter.[36]

The Illinois statute is different from the Maryland statue in some major ways. One difference is in the enforcement provision of the Illinois law. As mentioned above, Maryland's law does not have an enforcement provision whereas Illinois has a rather expansive enforcement scheme. Under Administration and Enforcement section of the Right to Privacy in the Workplace Act, an employee may file a complaint with the Director of Labor who is authorized to enforce this law.[37] The Director of Labor must first attempt to resolve the complaint via "conference, conciliation, or persuasion."[38] If this fails, the Director can bring an action in circuit court to compel compliance with the law. If the conference, conciliation or persuasion by the Director do not result them commencing action in circuit court, an employee may bring a civil action for injunctive relief and to recover actual damages plus costs. For a willful and knowing violation of this Act, the employee may recover $200 plus costs, reasonable attorney's fees, and actual damages. Any employer or prospective employer or his agent who violates the provisions of this Act is guilty of a petty offense and subject to a $1,000 fine.[39]

Another difference between the Maryland and Illinois law is that the Illinois law provides no specific exceptions. Instead of outlining specific exceptions as Maryland's law does, the law merely reiterates that it is not intended to restrict an employer's right to promulgate policies regulating use of the employer's own electronic resources or from monitoring usage of the employer's own electronic resources, including e-mail. However, the Illinois law and Maryland

[36] 820 Ill. Comp. Stat. 55/10(b)(4).
[37] *Id*.
[38] *Id*.
[39] *Id*.

law are similar in that they both do not have exceptions for an employer's legitimate workplace investigation. For example, imagine if an employee makes a death threat to a co-worker via a password protected social media page. As both laws are written now, it would appear that an employer is prevented from accessing the page unless an employee provides access voluntarily.

The Illinois law does expressly state that it does not apply to "information that is in the public domain."[40] Public domain most likely refers to social media sites for which the account holder has not used privacy settings to restrict access. However, this limitation provides little aid to employers as applicants and employees increasingly activate privacy settings to restrict access to their social media accounts. Furthermore, because the law does not provide any specific definition of "public domain nor does it imply what the scope of this phrase entails, it will likely result in expensive litigation in order to define the phrase. In the case of Facebook specifically, there are many different types of privacy settings that one may implement on their page. It is likely that someone who has no privacy settings and allows access to anyone on Facebook to view their page's information would qualify as having information in the "public domain." However, many people restrict their page's access to "Friends" or "Friends of Friends." Under this scenario, would a person's page still qualify as "public domain"? Would it matter if the person had seventy "Friends" verses seven hundred? These are all questions that will have to be answered in the courtroom.

There is additional troubling ambiguous language in the Illinois law. Specifically, it is unclear how the language prohibiting employer's ability to "demand access in any manner" will be interpreted.[41] For many social networking sites, someone needs to "request" to follow or become "Friends" with another. If a supervisor sends a "Friend Request" on Facebook would

[40] *Id.*
[41] *Id.*

this rise to the level of "demanding access in any manner?" It is difficult to believe that a request, that can be denied, is "demanding" yet there may be an argument that the employee felt compelled to accept the request or face retaliation at work.

California

On September 27, 2012, California signed into law the nation's third law prohibiting employers from requiring or requesting that an employee or applicant provide access to personal social media content.[42] The law is entitled "Employer Use of Social Media" and goes into effect January 1, 2013.[43]

California's law broadly prohibits employer's access to applicants and employees personal social media content. Employers cannot request or require that applicants or employees: "disclose social media log-in credentials, access personal social media in the employer's presence that is commonly referred to as called shoulder surfing, or "divulge any personal social media content."[44] The third prohibition is written in very broad terms, and looks to prevent an employer from asking an employee to provide the personal social media content of a co-worker who is Facebook friends with another employee.[45]

Under the law, "social media" is defined to include social media services and accounts, as well as content such as videos, photos, blogs, podcasts, test messages, email, and website profiles and locations. The bill also prohibits an employer from discharging, disciplining, threatening to

[42] S.B.1349, Gen. Assemb, Reg. Sess. (Cal. 2012).
[43] REUTERS.COM (Sept. 27, 2012), http://www.reuters.com/article/2012/09/27/us-usa-california-privacy-idUSBRE88Q1UI20120927.
[44] Philip Gordon and Lauren Woon, *California's New Social Media "Password Protection" Law Takes a More Balanced Approach by Accounting for Employers' Legitimate Business Interests*, (October 10, 2012), http://www.littler.com/publication-press/publication/californias-new-social-media-password-protection-law-takes-more-balanc.
[45] *Id.*

discharge or discipline, or otherwise retaliating against an employee or applicant for not complying with a request or demand for access to the employee's personal social media.[46]

The law has been criticized for being too vague in its language and thus overbroad in its eventual application.[47] One point of contention from these critics is the statutes' limited application to only "personal social media" and "personal social media information" without providing any guidance as to the definition of the word personal. The term "personal" can be especially problematic where a student or employee controls a business-related or quasi-business-related social media account. For example, in the case of Facebook, a student can have administrative privileges over the page of a product, brand, or service. Furthermore, distinguishing between "personal" and "business-related" social media accounts will certainly be a source of major litigation. For example, it is unclear if a Facebook or Twitter account of a prominent blogger would be considered a "personal social media account." Another factor that may come into play in this determination is the privacy settings on the account. Either way, the California courts will initially have to struggle with these and similar questions as they attempt to define the term "personal." Unfortunately, depending on how California courts answer these questions, it may severely limit the effectiveness of the new laws as envisioned by the California legislature.

The California law differs from the Illinois and Maryland laws with a critical exception for employers, which fosters more of a balancing for employer's interests. An employer can request an employee to divulge personal social media passwords reasonably believed to be

---

[46] *See Supra* note 41.

[47] Eric Goldman, *Big Problems in California's New Law Restricting Employers' Access to Employees' Online Accounts*, FORBES.COM, (Sept. 28, 2012), http://www.forbes.com/sites/ericgoldman/2012/09/28/big-problems-in-californias-new-law-restricting-employers-access-to-employees-online-accounts/.

relevant to an investigation of allegations of employee misconduct or violation of laws and regulations. An employer can only use the information obtained via this exception "solely for purposes of that investigation or a related proceeding."[48] Thus, in the hypothetical raised earlier where an employee makes a death threat via a password protected social media site, under California law the employer would be allowed access to this information if reasonable believed to be relevant to an investigation of employee misconduct. Also, the statute does not prevent employers from requiring that employees disclose usernames and passwords for the purpose of accessing employer-issued electronic devices.

However, as with the Maryland statute, the California law has a problematic enforcement provision. In order for an employee to bring a suit alleging a violation of this statute they must bring their claim to the California Labor Commissioner. However, what happens to the employees claims if the California Labor Commissioner declines to investigate their alleged violation is unknown.[49] The law specifically states that the Labor Commissioner is not required to investigate complaints that the law had been violated. Furthermore, the law does not create a private right of action for an employee to prosecute violations of the law.[50]

California also has signed into law a companion statute which makes it illegal for colleges and universities to demand social media user names and passwords from students and prospective students.[51] This bill does not affect an institution's existing ability "to protect against

---

[48] *See Supra* note 41.
[49] *Id.*
[50] *Id.*
[51] Megan Garber, *In California, It's Now Illegal for Employers and Universities to Ask for Your Social Media Passwords,* THEATLANTIC.COM, (Sept. 28, 2012), http://www.theatlantic.com/technology/archive/2012/09/in-california-its-now-illegal-for-employers-and-universities-to-ask-for-your-social-media-passwords/262990/.

and investigate alleged student misconduct or violations of applicable laws and regulations."[52] This bill will also go into effect on January 1, 2013.

New Jersey

On October 25, 2012 the New Jersey Senate gave the final legislative approval to a measure that prevents employers from asking job applicants and employees for their social media passwords.[53] Additionally, employees would be protected from retaliation or discrimination should they refuse to disclose their password or log-in information, file a complaint pursuant to this bill, or testify, assist or participate in any investigation concerning a violation of this law.[54] Employers would even be prohibited from requiring or requesting that the employee disclose whether he or she has a social media account.[55]

The New Jersey legislation is different from the aforementioned Maryland, Illinois, and California statutes in its enforcement provision. The New Jersey law provides for a private cause of action for prospective, current, and former employees for appropriate damages and injunctive relief, including attorneys' fees. Employees aggrieved by the bill can also file a complaint with the New Jersey Department of Labor and Workforce Development, which would be authorized to impose civil penalties of $1,000 for the first violation or $2,500 for each subsequent violation.[56]

---

[52] Wyatt Buchanan, *Brown signs social-media passwords bill*, SAN FRANCISCO CHRONICLE, (Sept. 27, 2012), http://www.sfgate.com/bayarea/article/Jerry-Brown-signs-bill-on-social-media-passwords-3900109.php.
[53] Kibret Markos, *N.J. Senate set to vote on bill that would ban employer demands for social media access*, NORTHJERSEY.COM, (Oct. 24, 2012), http://www.northjersey.com/news/NJ_Senate_to_consider_bill_to_ban_employer_demands_for_social-media_access.html?page=all.
[54] A-2878, N.J. ASSEM., (2012), *available at*, http://www.njleg.state.nj.us/2012/Bills/A3000/2878_I1.HTM.
[55] *Id*.
[56] *Id*.

Some legal practitioners have been critical of the enforcement provision of this bill.[57] Since this bill is unique in creating a private cause of action, critics argue that the legislature should have given specific guidance to the standards for bring a suit under this statute. Many potential questions arise from this newly created private right of action specifically questions as to what exact elements an aggrieved party would have the burden of proving to succeed on its claims. Would the party have to prove that they would have been hired but for their granting of their social media password? Another problematic provision is that a party may seek injunctive relief, which would require an employer to hire an employee that they originally expected not to make an offer to. [58]

Critics have also pointed to the particularly broad provision of the law that would prohibit an employer from requiring an employee or applicant to provide the employer with "access" to the individual's social-networking site "in any way" as problematic. This language would seem to prevent more employer conduct than the "demanding access in any manner" language in the Illinois statute. When this language is combined with the fact that employers are prevented from even asking if an employee has a social media account, it would seem as though the statute would prevent a supervisor from sending a Facebook friend request or an invitation to connect via LinkedIn to an employee.

Just like California, New Jersey also passed a companion bill preventing colleges and universities from requiring a student or applicant to provide or disclose any user name, password or other means for accessing a personal account through an electronic communications device. The bill, allows for an aggrieved party to bring a civil action seeking injunctive relief,

---

[57] Paulette Brown, *Flawed Social-Media Bill Goes Far Beyond Protecting Privacy*, NJ LAW JOURNAL, (Nov. 20, 2012), http://www.law.com/jsp/nj/PubArticleNJ.jsp?id=1202578994297&slreturn=20121030084155.

[58] *Id*.

compensatory and consequential damages, and reasonable attorney fees. Although one difference from its companion bill is that it does not result in a fine against the colleges within violation.[59]

The Legal Risks of Employer's Using Social Media to Research Potential Employees

As helpful as the above state and federal statutes might be in preventing employers from demanding access to an employee's password protected social media account, there are some existing laws which certainly serve as a disincentive for employer's to desire this access. The following will analyze these laws and discuss their ability to be a valid disincentive to employer's, which might negate the need for state or federal legislation.

Stored Communications Act Liability

The Stored Communications Act of 1986 ("SCA") makes it unlawful to "(1) intentionally access without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed an authorization to access that facility . . . and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage."[60] A couple cases have ruled that an employer who gains unauthorized access to an employee's password-protected social media account and subsequently punishes or fires the employee for anything appearing on that account, may have violated the SCA and thus would be liable to the employee for that unauthorized access.[61]

In *Konop v. Hawaiian Airlines, Inc.*, the plaintiff, Robert Konop, an airline, pilot sued his supervisors under the SCA.[62] Konop alleged that this supervisors had looked at his password-protected website without authorization and divulged information found on the website to

---

[59] A-2879, N.J. ASSEM., (2012), *available at,* http://www.njleg.state.nj.us/2012/Bills/A3000/2879_I1.HTM.
[60] 18 U.S.C. §§ 2701-2711 (2000 & Supp. I 2001).
[61] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002); *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754 (FSH), 2008 WL 3128420, at *2 (D.N.J. July 25, 2008).
[62] *Konop*, 302 F.3d 868 (9th Cir. 2002).

others.[63] Konop created the web site because he was upset at his union and posted on the site statements criticizing defendant's President and urging his co-workers to consider alternative union representation.

Konop's site was not open to the general public. To gain access to the site, one had to input an assigned user name, which Konop gave only to selected Hawaiian employees. User names were not given either to Hawaiian's management or to his union. Once the user entered his user name, he was presented with the site's terms and conditions, which he had to agree to honor before he would be given the password necessary to access the site. These terms included an agreement not to disclose the contents of Konop's site. If the user agreed to these terms, he was granted access to the site.[64]

James Davis was Hawaiian Vice President to whom Konop did not assign a user name, and who accordingly was not granted authorization by Konop to access the site. However, to obtain access, Davis contacted another Hawaiian pilot, who had been granted a user name but had never accessed the site. This pilot gave Davis his user name, which Davis then used to access the site.[65] Konop contends that Davis thereafter disclosed the contents of the site to both Hawaiian's President and the union. A representative of the union thereafter contacted Konop and informed him that Hawaiian's President was upset with the contents of the site.

The Ninth Circuit held that one who views the contents of a password-protected web site without permission of the site owner could be found to violate the SCA. The SCA provides a liability exception that "allows a person to authorize a third party's access to an electronic communication if the person is (1) a 'user' of the 'service' and (2) the communication is 'of or

---

[63] *Id.*
[64] *Id*. at 872–73.
[65] *Id*.

intended for that user."[66] The Ninth Circuit reasoned that the pilot who gave the Vice President his user name information was not a "user" and therefore could not grant access to the vice president without violating the SCA. The pilot was not believed to be a "user" of Konop's website because he had never accessed the website before.[67]

The Ninth Circuit's holding seems to imply that an employer not expressly granted access to an employee's website could still gain legal access if another employee who actually uses or views the website supply them with their account information. However, a few years later a district court in New Jersey was confronted with this exact situation. In *Pietrylo v. Hillstone Restaurant Group*, Brian Pietrylo, a restaurant server, was unhappy about his working conditions. [68] Pietrylo then created a chat group for employees and former employees on MySpace.com, accessible by invitation only and the chat group was password protected.[69] Pietrylo stated that the purpose of the group was "to vent about any BS we deal with [at] work without any outside eyes spying in on us."[70]

One day, Karen St. Jean, a coworker of Pietrylo and a member of his MySpace group, was dining at the home of one of the restaurant managers. While dining, St. Jean told the manager about the chat group on MySpace. Later, St. Jean was asked by another manager for her password to view the MySpace page, which she complied with. St. Jean testified that she "felt that [she] probably would have gotten into trouble," if she had not given the password. Several managers then accessed and monitored the chat group on a number of occasions. Managers observed many unprofessional comments from employees including sexual remarks and

[66] 18 U.S.C. § 2510(13) (2006).
[67] *Konop*, 302 F.3d 880 (9th Cir. 2002).
[68] *Pietrylo*, 2009 WL 3128420, at *1.
[69] *Id.* at 1.
[70] *Id.*

references to violence and drug use. Pietrylo was soon fired and subsequently sued the restaurant alleging, among other things, a violation the SCA.

A jury found that the restaurant had violated the SCA and awarded damages, including punitive damages to Pietrylo. The defendants moved for a judgment as a matter of law, arguing that there could be no SCA violation if access was authorized "by a user of that service with respect to a communication." Since St. Jean was a user and gave her password to the managers, the restaurant argued that St. Jean authorized their use and thus there was no violation.[71]

The New Jersey court denied their motion. There was plenty of evidence for the jury to conclude that St. Jean was acting under duress and that the managers "knew that they were not actually authorized to continue to access the [chat group] through [St. Jean's] MySpace password, but continued to do so anyway."[72] Thus, the court in its reasoning highlighted that the key to an SCA violation would be valid "authorization."

Consequently, outside bringing suit via one of the state and federal statutes previously discussed, the SCA may provide an employee with a cause of action against his or her employer if an employer gains unauthorized access to the content by coercing an authorized user for their log-in information. So, if the employees in *Kopono* and *Pietrylo* had invited their managers to join their password protected group, then they would have no claim under the SCA. Using this logic, one can imagine a court relying on this precedent to hold that an employer who is "Friends" on Facebook with their employees would have authorized access to the employee's Facebook page.

Computer Fraud and Abuse Act

[71] *Id.* at *3.
[72] *Id*.

Section (2)(C) of the Computer Fraud and Abuse Act ("CFAA") prohibits a person from "intentionally access[ing] a computer without authorization" and thereby obtaining "information from any protected computer."[73] Section (5)(C) makes it an offense if one "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."[74] The CFAA broadly defines "computer," and extends the reach of the section to any "protected computer" which is "used in or affecting interstate or foreign commerce."[75]

In *Eagle v Morgan,* Linda Eagle, former CEO of Edcomm, Inc. (Edcomm"), filed a complaint in the U.S. District Court in Pennsylvania alleging that Edcomm stole her LinkedIn social media account in violation of the CFAA after she was terminated. While Eagle was the CEO of Edcomm, she established a LinkedIn account and that she used to promote Edcomm's banking education eservices, to foster her reputation as a businesswoman, to reconnect with family, friends and colleagues, and to build social and professional relationships. Edcomm employees assisted Eagle in maintaining her LinkedIn account and had access to her passwords. Edcomm encourages all employees to participate in LinkedIn and contended that when an employee left the company, Edcomm would effectively "own" the LinkedIn account and could "mine" the information and income traffic.[76]

After Eagle was terminated, Edcomm, using Eagle's LinkedIn password, accessed her account and changed the password so that Eagle could no longer access the account and then changed the account profile to display Eagle's successor's name and photograph, although Eagle's honors, awards, recommendations, and connections were not deleted. Eagle contended that Edomm's actions violated the CFA, Section 43(a) of the Lanham Act and numerous state

[73] 18 U.S.C. § 1030(a)(2)(C).
[74] 18 U.S.C. § 1030(a)(5)(C).
[75] 18 U.S.C. § 1030(e)(2).
[76] Eagle v. Morgan, CIV-No. 11-4303, 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012).

and common laws. In an October 4, 2012 ruling on the company's summary judgment motion, U.S. District Judge dismissed Eagle's CFAA and Lanham Act claims against Edcomm but held that Eagle had the right to a trial on whether Edcomm had violated state misappropriation law and other state laws.

In rejecting Eagle's CFAA claim, the court set a high bar for future private plaintiff's claiming injury under this statute. The court rejected Eagle's CFAA claim because Eagle could not show adequate damages under the statute. According to the court, a legally cognizable "loss" under the CFAA requires "impairment or damage to a computer or computer system," or at least "lost revenue resulting from an interruption of service or the inoperability of computers." Mere allegations of harm to an ongoing business are insufficient. Here, the plaintiff had presented evidence that she had "missed out" on professional opportunities because of her inability to access the LinkedIn account. Thus, her allegations of loss were "pure conjecture."[77]

Although this case does not yet provide a clear understanding of the extent to employer's rights of social media, it is clear that both employers and employees must be aware of their actions. Additionally, it shows that LinkedIn by its very nature may arguably create property rights that are valuable to employees and employers alike. Employers may view employees' social media accounts as a potential repository of proprietary information, especially customer contacts.

Discrimination Liability

Title VII of the Civil Rights Act as well as similar state laws prohibiting discrimination and harassment protect job applicants and employees. Specifically, Title VII prohibits

[77] *Id.*

discrimination on the basis of race, color, religion, sex, or national origin.[78] The Equal Employment Opportunity Commission ("EEOC") enforces Title VII's antidiscrimination and antiharassment laws.[79]

The vast majority of social network users post private information online using social media outlets such as Facebook or LinkedIn. On Facebook alone, a user can broadcast their sexual orientation, relationship status, religious beliefs, and political affiliations. Thus, although it may be advantageous for an employer to use social media as a background check, it may expose the employer to information of the candidate's race, religion, or other protected class that employers are legally barred from using in the hiring process. This is exactly the situation that the University of Kentucky recently found itself in.

In *Gaskell v University of Kentucky*, the university was the target of a Title VII claim after it failed to hire a job applicant for a position as director of the university observatory.[80] The university admitted that the plaintiff had more education and experience than the person hired for the position but asserted the person hired had demonstrated more of the qualities it wanted for the position. The plaintiff, on the other hand, claimed he was rejected for the position because of his expression of his religious beliefs. The plaintiff claimed that during the hiring process, one of the hiring committee members conducted an Internet search and came across the plaintiff's personal website that contained an article he had written about the Bible evidencing the plaintiff's evangelical Christian faith and belief in creationism. There was evidence that the

[78] 42 U.S.C. §§ 2000e *et seq*.
[79] 42 U.S.C. § 2000e-4.
[80] Gaskell v. University of Ky., 2010 U.S. Dist. LEXIS 124572 (E.D. Ky. Nov. 23, 2010).

search committee brought his article to the biology department, which expressed concerns over the plaintiff's belief in creationism.[81]

The court denied cross-motions for summary judgment, finding the arguments very fact-intensive.[82] The case was eventually settled before trial for 125,000.[83] Although the case settled, it is instructive in shedding light on the potential ramifications of using the Internet or social media to research job applicants. Furthermore, a more recent case shows how even the mere existence of social media information can support a discrimination claim.

In Illinois, a *pro se* plaintiff, Jason Nieman, brought to federal court an age discrimination claim against his employer.[84] Nieman suggests that his employer was aware of his age based on the inclusion of the year he graduated from college in his LinkedIn profile. The court denied the employer's motion to dismiss, allowing Nieman's claims to continue, reasoning that it is "not difficult to determine that someone who graduated from college in 1989 probably was over the age of 40 in 2010."[85]

Tortious Interference with Contract

Facebook has expressed their opinions on the issue of whether employers should be researching their potential hires using Facebook. Erin Egan, Facebook's chief privacy officer, released a statement objecting to this practice on both legal and ethical grounds.[86] Egan asserts that "as a user, you shouldn't be forced to share your private information and communications

---

[81] *Id.*
[82] *Id.* at 29-30.
[83] Dylan Lovan, *University of Kentucky Settles Suit With Astronomer Martin Gaskell*, HUFFINGTON POST, (Jan.18, 2011), http://www.huffingtonpost.com/2011/01/18/university-of-kentucky-se_n_810540.html.
[84] Nieman v. Grange Mut. Cas. Co., 11-3404, 2012 WL 1467562 (C.D. Ill. Apr. 27, 2012).
[85] *Id.* at 2.
[86] Erin Egan, *Protecting Your Passwords and Your Privacy*, FACEBOOK.COM, (March 23, 2012), http://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057.

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."[87] Facebook has expressly prohibited "solicit[ing] login information or access[ing] an account belonging to someone else."[88] Furthermore, Facebook clearly states in its Statement of Rights and Responsibilities that the user "shall not share [their] password...[or] let anyone else access [their] account."[89]

Thus, an employer who requests an applicant's Facebook password would be compelling the applicant to violate Facebook's terms and conditions. Any first-year law student would recognize this as a potential tortious interference with contract. Tortious interference with contract occurs when one intentionally and improperly interferes with the performance of a contract (except a contract to marry) between another and a third person by inducing or otherwise causing the third person not to perform the contract, is subject to liability to the other for the pecuniary loss resulting to the other from the failure of the third person to perform the contract.[90]

The job applicant has entered into a contract with Facebook when they click to accept (probably without reading) Facebook's terms and conditions. Hence, an employer who asks the employee for their social media password is causing the applicant to break the terms of his or her contract with Facebook. However, a lingering problem is whether or not the breaking of this term results in any pecuniary loss to the applicant. Demonstrating pecuniary loss may be difficult to prove; nevertheless this theory of liability seems to be implicated in this factual scenario.

---

[87] *Id.*
[88] *Statement of Rights and Responsibilities,* Facebook, http://www.facebook.com/legal/terms (last updated June 8, 2012).
[89] Facebook, *supra* note 86.
[90] Restatement (Second) of Torts § 766 (1979).

Conclusion

It is rarely argued that employer's should absolutely have a right to access your password protected social media page when you are applying for a job. The real question is whether state and federal legislators are necessary to protect employees from these offensive practices. As analyzed above, many of the state legislations are overbroad, provide little exceptions, and do not take into account employer's legitimate business interests. The legislations are also filled with ambiguous language, which undoubtedly will result in a great deal of litigation. Yet most problematic is the lack of enforcement power most of the state legislations provide in not affording a private cause of action for aggrieved parties.

Additionally, employers may have enough of an incentive to not demand employer's passwords based on existing statutes. The SCA may prove the most protection to employees if it can provide a private cause of action for invasion of privacy based on coerced disclosure of a password-protected account. However, a CFAA violation for unauthorized access to a protected computer did not seem to persuade the judge in *Eagle* and the Title VII liability is still largely untapped. Thus, it remains to be seen whether the new state and federal legislation will be helpful or merely muddy the already opaque waters of employees and employers social media rights.