Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.142

http://tlp.law.pitt.edu

Too Much Too Soon? A Case for Hesitancy in the Passage of State and Federal Password Protection Laws

Megan Davis

Too Much Too Soon? A Case for Hesitancy in the Passage of State and Federal Password Protection Laws

Megan Davis*

INTRODUCTION

In May of 2012, Maryland Governor Martin O'Malley signed into law the nation's first employee social media privacy protection law banning employers from requiring applicants and employees to provide them with login information to their social media accounts as a term of receiving or keeping employment.[1] Since then, twelve other states have followed Maryland's lead and either enacted or initiated the process of enacting some form of law aimed at prohibiting employers from gaining access to a candidate's private social media information.[2]

These actions come after widespread public outrage at personal stories of employers requesting and/or requiring unlimited access to applicants' and employees' social media accounts, including information kept private such as Facebook's private messaging service.[3] In a press release on the subject, Senator Richard Blumenthal (D-CT) said,

> I am alarmed and outraged by rapidly and widely spreading employer practices seeking access to Facebook passwords or confidential information on other social networks. A ban on these practices is

* Juris Doctor Candidate, Class of 2015, at the University of Pittsburgh School of Law. The author would like to thank everyone on the staff and editorial board of the *Pittsburgh Journal of Technology Law and Policy* for their support throughout the writing process. Special thanks to Kevin Leary, Elizabeth Orton, Chris Schlag, and Kevin Rogers for their guidance and insightful critique. Finally, the author would like to thank her friends and family, all of whom have been instrumental to her success on the Journal and in all aspects of her law school career.

[1] Melissa Coretz Goemann, *Maryland Passes Nation's First Social Media Privacy Protection Bill*, ACLU (May 4, 2012, 4:30 PM), https://www.aclu.org/blog/technology-and-liberty/maryland-passes-nations-first-social-media-privacy-protection-bill.

[2] *See* Michelle Poore, *Law & Informatics Symposium on Labor and Employment Issues: Article: A Call for Uncle Sam to Get Big Brother Out of Our Knickers: Protecting Privacy and Freedom of Speech Interests in Social Media Accounts*, 40 N. KY. L. REV. 507, 508 (2013).

[3] *See* Goemann, *supra* note 1.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

> necessary to stop unreasonable and unacceptable invasions of privacy.[4]

The practice of asking employees and potential employees for social media login information, when implemented, raises a variety of complex legal issues. State and federal lawmakers have jumped at the opportunity to disparage the exercise; at the time of publication of this note, the Social Networking Online Protection Act ("SNOPA") has been referred to a Congressional committee to determine the appropriateness of introducing the bill into Congress.[5] At the state level, twenty-six states have implemented or have introduced legislation that would ban or regulate the practice.[6]

Despite this national indignation, the extent of this legislative frenzy is both unwarranted and dangerous given the general lack of reliable information available. The proper balance between legitimate employer needs and an applicant's or employee's right to privacy and equal protection is unclear and is not a question that should be answered through rushed legislation. It is important to note that in addition to the wide variance in protections offered in the state statutes that have already been enacted, which can lead to confusion amongst employers and employees regarding legal rights and responsibilities, a number of legal remedies are already available to protect privacy interests in social media content.[7] Additionally, even though determining exactly what conduct should be outlawed seems like a simple task, in practice it can be extremely arduous. While banning employers from requiring usernames and passwords may be a fairly straightforward objective, an employer's cyber-vetting of hopeful employees can take on other, more nebulous forms. For example, when is it unlawful for an employer to examine an applicant's Facebook page? Only while in his or her presence? When is it acceptable for an employer to "friend" an applicant prior to making an employment decision? Or for an employer to use a third-party application in conducting social media checks? The practical difficulties associated with creating an effective social

---

[4] *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. 26, 2012), http://www.schumer.senate.gov/Newsroom/record.cfm?id=336396.

[5] *See H.R. 537: Social Networking Online Protection Act*, GOVTRACK, https://www.govtrack.us/congress/bills/113/hr537#overview (last visited Mar. 1, 2014) (noting that after the Bill was introduced on February 6, 2016, it progressed through to the reference committee).

[6] *See Employer Access to Social Media Usernames and Passwords*, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last modified Feb. 21, 2014) (providing descriptions of the various state password protection laws and their status).

[7] *See* discussion *infra* Part III.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

media protection law manifest themselves in the vast differences in protection allowed under the various state laws currently in place. While some of these laws provide a liberal amount of protection for hopeful employees, others provide only a bare minimum.[8]

The purpose of this note is to advocate for a more hesitant legislative stance toward social media password protection laws in an effort to avoid unnecessarily over-legislating in an area of privacy law that is still developing. While an outright rejection of such legislation is not intended, the speed and political vigor with which lawmakers are moving forward with such statutes raises the risk of statutory ambiguity, confusion amongst affected parties, and unnecessary burdens on employers, not to mention one more concern for lawmakers who are busy drafting legislation to deal with other equally important societal issues. Part I of this note outlines the various reports identifying the trend in employers asking for social media login information, in an effort to discern how widespread the practice actually is, as well as what form these requests take. Part II provides an analysis of the current legal regime, which includes the Fair Credit Reporting Act ("FCRA"), the Federal Stored Communications Act ("SCA"), employee protections under the National Labor Relations Act ("NLRA"), Title VII's anti-discrimination prohibitions, and the constitutional protection provided by the Fourth Amendment of the U.S. Constitution. Part II will also show the strengths and weaknesses each of these protections provide and highlight some of the functional limitations of each. Part II concludes that the current legal regime is sufficient to protect against some, but not all, of the problems password protection laws seek to remedy, thereby making many of these laws redundant, time-consuming, and unnecessary. Part III outlines the practical difficulties in drafting a sufficiently narrowly tailored social media privacy law, including disparities in the statutes of those states that have chosen to enact laws safeguarding private social media accounts and defining appropriate exceptions for legitimate employer interests, such as investigating harassment claims and avoiding liability under negligent hire laws.

I. THE PERVASIVENESS OF THE ISSUE: WHAT WE KNOW AND WHAT WE DON'T

The debate regarding social media password protection began in 2011 when Mr. Robert Collins contacted the ACLU of Maryland, outraged by the fact that he had been required to hand over his Facebook password and username in order to

[8] *Employer Access to Social Media Usernames and Passwords*, *supra* note 6.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

reapply for a job with the Maryland Department of Corrections.[9] As more individuals came forward confirming Collins' statement with their own personal stories, privacy advocates from across the country began to vocalize their opposition to the practice.[10]

Potential employees are often warned about the dangers of posting controversial content on social media sites and therefore should know the risk that a potential employer might see that publicly available information.[11] Studies are inconclusive on exactly how frequently public content is accessed in making hiring decisions. For example, one survey indicates that forty-five percent of employers access public social media content when making hiring decisions,[12] while another study indicates that the number may be closer to seventy-five percent.[13] No matter what the percentage, the fact remains that any content posted to a public social media account can be accessed by just about anyone, including potential employers.[14]

The issue of how many employers actually require login information in order to access private information is not nearly as well researched. Out of the few reputable studies available, only one study conducted by the Associated Press actually pointed to one unnamed private company that required at least one applicant to provide it with a Facebook password.[15] Outside of that, there was little evidence that this is a common practice in the private employment sphere.[16] That being said, there were a few instances of private employers using less invasive, but still questionable, techniques such as having an applicant log in to their social media profiles in the presence of an interviewer or asking the applicant to "friend"

---

[9] *See* Goemann, *supra* note 1.

[10] *Id.*

[11] *See* Poore, *supra* note 2.

[12] Rosemary Haefner, *More Employers Screening Candidates via Social Networking Sites*, CAREERBUILDER, http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/?ArticleID=1337 (last modified June 10, 2009).

[13] Jennifer Preston, *Social Media History Becomes a New Job Hurdle*, N.Y. TIMES (July 10, 2011, 12:00 AM), http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html?pagewanted=all&_r=0.

[14] *See* Poore, *supra* note 2.

[15] The Associated Press, *Senators Question Employer Requests for Facebook Passwords*, N.Y. TIMES, Mar. 25, 2012, 12:00 AM, http://www.nytimes.com/2012/03/26/technology/senators-want-employers-facebook-password-requests-reviewed.html.

[16] Matthew Kauffman, *Claim Check: Employers Asking for Facebook Passwords*, HARTFORD COURANT (Mar. 27, 2012, 12:00 AM), http://courantblogs.com/investigative-reporting/claim-check-employers-asking-for-facebook-passwords/.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

the interviewer.[17] All other examples came from the public employment sphere in primarily the area of law enforcement where invasive background checks involving psychological examinations are a common practice.[18] The authors of the Associated Press study never purported to claim that the practice is widespread, nor did they claim that the practice is growing in popularity.[19]

The general lack of information available to support the rush towards increased privacy legislation should at the very least cause some hesitancy amongst lawmakers and potentially affected parties regarding the necessity of these legislative efforts. When added to the established protections afforded by other laws already in place, the reasons for this skepticism become more apparent.

II. THE CURRENT LEGAL REGIME

As is historically common, the legal sphere has yet to catch up to the technological advances of recent years, and social media is no exception.[20] Many of the laws that are currently utilized in cases regarding misuse of social media sites and profiles were drafted well before the advent of modern social media.[21] This does not mean, however, that those whose rights have been violated in some way are left completely without redress.

A. Anti-Discrimination Laws

While employers in many states are not currently outlawed from requesting an employee's social media login information, those employers are prohibited from discriminating against employees based on much of the information their social media pages provide.[22] One area that provides a breeding ground for potential litigation when social media becomes involved is the potential employee background check.[23]

---

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] Michelle Scheinman, *Labor: Chapter 618: Cyberfrontier: New Guidelines for Employers Regarding Employee Social Media*, 44 MCGEORGE L. REV. 731, 732 (2013).

[21] *See* discussion *infra* pts. III(a), III(b), III(c), III(d), and III(e).

[22] Megan Whitehill, Comment, *Better Safe Than Subjective: The Problematic Intersection of Pre-Hire Social Networking Checks and Title VII Employment Discrimination*, 85 TEMP. L. REV. 229, 232 (2012).

[23] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

While background checks on potential employees are nothing new, the cyber-vetting trend that has emerged in recent years differs substantially from more traditional practices.[24] Traditionally, background checks consisted of a screening of criminal records, credit scores, civil judgments against the candidate, and other officially determined criteria, the analysis of which does not involve a great deal of subjectivity.[25] These factors can also easily be challenged should an applicant feel that their background check was inaccurate.[26] Social media checks, on the other hand, necessarily require an employer to evaluate private information that can easily be taken out of context or misunderstood.[27] With no official determination or explanation of the information an employer might find on a social media account, employers are free to utilize a great deal of subjectivity in determining whether such fragmented information indicates how well the employee would fit within the organization.[28]

The subjectivity inherent in cyber-vetting practices creates a variety of legal risks for employers, especially when it comes to determining if a Title VII hiring discrimination has taken place.[29] Title VII of the Civil Rights Act of 1964 makes it illegal for an employer "to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual . . . because of such individual's race, color, religion, sex or national origin."[30] It is Title VII that prevents an employer from asking questions related to an applicant's protected status during a job interview or seeking out information that would help an employer determine if the applicant did in fact fall into such a class.[31] An employer can avoid liability under Title VII if it can prove it had no knowledge of the applicant's status as a member of a protected class.[32]

In proving a Title VII discrimination claim, an affected potential employee must show that he or she was within a protected class, was qualified for the

---

[24] Dr. Shaby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 554 (2013).

[25] *Id.*

[26] *Id.*

[27] Ghoshray, *supra* note 24, at 562.

[28] *Id.*

[29] Whitehill, *supra* note 22, at 253.

[30] Civil Rights Act of 1964, 42 U.S.C. § 2000(e)-2(a)(1) (2012).

[31] Whitehill, *supra* note 22, at 229, 253.

[32] *Id.* at 252.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

position, met the employer's legitimate performance expectations, was adversely affected, and the evidence presented is sufficient to give rise to an inference of discrimination.[33] Discriminatory intent need not be the sole reason behind a decision not to offer a particular applicant a position because the United States' Supreme Court has recognized a mixed-motive claim for discrimination, which holds that an employer may not consider any protected factors in making an employment decision.[34] This is true even if the protected trait was considered alongside legitimate factors and even if the ultimate determination would have been the same had the protected trait not been considered.[35]

A determination that the evidence on record is sufficient to support an inference of discrimination is most often shown through the introduction of circumstantial evidence.[36] One piece of evidence that is often considered is the amount of subjectivity allowed in the hiring process.[37] While it is not unlawful to use subjective practices in hiring determinations per se, the greater the level of subjectivity utilized in a company's hiring processes, the more likely a court will find that discrimination has taken place.[38]

Limiting the level of subjectivity that takes place during hiring procedures is not an easy task, but if an employer is truly dedicated to avoiding discrimination litigation, there are a few practices these employers can and will likely implement to show their dedication to objective hiring. First, employers can implement practices that create exposure control.[39] Exposure control mechanisms seek to prevent those in charge of hiring from coming across information that could potentially expose an applicant's protected status by limiting the information such hiring managers receive during the interview process.[40] For example, hiring managers could be required to decide which applicants to interview based solely on the content of resume submissions, with no additional background checks or

[33] *See* McDonnell Douglas Corp. v. Green, 411 U.S. 792, 802–05 (1973).

[34] Price Waterhouse v. Hopkins, 490 U.S. 228, 241 (1989).

[35] *Id.*

[36] Whitehill, *supra* note 22, at 239, 242–43.

[37] *Id.* at 243.

[38] Turner v. Public Serv. Co. of Colo., 563 F.3d 1136, 1145 (10th Cir. 2009).

[39] Whitehill, *supra* note 22, at 257.

[40] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

investigations.[41] The less likely an employer is to know about an applicant's protected trait, the less likely that employer will become subject to litigation.[42]

Second, subjectivity can be limited by implementing a process for exclusively objective evaluations.[43] Exclusively objective evaluations require that hiring managers base their decisions solely on objectively determinable factors, such as grade point average, years of experience in the field, etc.[44] Such practices take the power away from those in charge of hiring and eliminate the opportunity for any improper biases to enter the realm of hiring decisions.[45]

The practice of cyber-vetting raises some obvious explicit and implicit discrimination issues. Social media accounts, whether they have been made private or public, often contain information that would identify an applicant as a member of a protected class, such as religious affiliation, gender, and/or race.[46] When an employer makes the choice to access an applicant's social media accounts, it rids itself of any ignorance of the applicant's status. Consequently, if an employment discrimination claim arises, the employer can no longer avoid liability by claiming it had no knowledge of the plaintiff's protected status.[47]

Additionally, as noted earlier, the practice of choosing applicants based on information from their social media profiles is highly subjective in nature. While such subjectivity is not necessarily illegal, the lack of any objective standards for reviewing such information is highly suspect and creates a significant risk of heightened scrutiny for employers in terms of discrimination litigation.[48] The desire to avoid a costly and publicity-ridden litigation process can prevent employers from choosing applicants based on what they post on social media profiles, either for public consumption or for private viewing, due to their knowledge that there is no objective criteria with which to analyze such information. The significance of this deterrence should not be overlooked in analyzing the current state of social media privacy protections.

---

[41] *Id.* at 258.

[42] *Id.* at 260.

[43] *Id.* at 257.

[44] *Id.*

[45] *Id.*

[46] Whitehill, *supra* note 22, at 254.

[47] *Id.* at 253.

[48] *Id.* at 252.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

B. The Stored Communications Act

The Stored Communications Act ("SCA"), a subset of the broader Electronic Communications Privacy Act ("ECPA"), criminalizes "intentional, unauthorized access to stored electronic communications held by an electronic communication service [and] . . . prohibits electronic communication services providers and remote computing services providers from disclosing user communication."[49] For the purposes of the SCA, an "electronic communication" means any transfer of data, such as text or images that occur via wire, radio or electronic system,[50] and an "electronic communications service" is a service that provides users the ability to send and receive electronic communications.[51] Section 2701 of the SCA, the section at issue for the purposes of this note, does not differentiate between public and private information.[52] It does, on the other hand, differentiate between "authorized" and "unauthorized" access to electronic communications, as authorization acts as a defense to a claim for violation of the SCA.[53]

There has been some question as to whether or not a law enacted in 1986 could adequately protect the privacy rights unique to more modern social media sites; after all, at the time of its enactment, the concept of social media as it is known today surely was not on the minds of those who drafted the law.[54] While the Supreme Court has yet to decide the issue, two recent federal district court decisions have held that the SCA does in fact apply to unauthorized access to private social media accounts, thereby opening the door to further discussion on the merits of utilizing this law in the context of employee social media use.[55]

In *Ehling v. Monmouth-Ocean Hospital Service Corp.*, the District Court of New Jersey found that the SCA protects a Facebook user's private pages (i.e. pages only visible to "friends").[56] The court in this case was called upon to decide if an

---

[49] The Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012).

[50] 18 U.S.C. § 2510(12).

[51] *Id.* at § 2510(17).

[52] 18 U.S.C. § 2701(a).

[53] *Id.* at § 2701(c).

[54] Todd C. Taylor, *Social Media and the Stored Communications Act: Does a 1986 Law Protect Timelines and Tweets?*, BLOOMBERG SOCIAL MEDIA LAW & POLICY REPORTS (Nov. 26, 2013), *available at* http://www.mvalaw.com/assets/attachments/Taylor%20Todd_Bloomberg%20BNA_Social%20Media%20SCA_11.26.13.pdf.

[55] Ehling v. Monmouth-Ocean Hospital Service Corp., No. 2:11-cv-03305, 2013 BL 220816 (D.N.J. Aug. 20, 2013); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 981–82 (C.D. Cal. 2010).

[56] *Ehling*, 2013 BL 220816, at *7.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

employee, Ms. Ehling, had been temporarily suspended from her employment improperly when her employer was alerted to postings on her Facebook wall that were only visible to her Facebook friends, but which the employer deemed inappropriate.[57] The employer learned about these postings from another employee of the organization that also happened to be Ms. Ehling's Facebook friend.[58] In deciding that Ms. Ehling's employer had accessed her postings in violation of the SCA, the court held that Facebook posts constitute "electronic communications" within the statutory definition as they involve sending data from a computing device to Facebook's servers, and that Facebook constitutes an "electronic communication service" because it's main purpose is to allow people to transmit and share data on its servers via the Internet and posts are stored indefinitely for archiving purposes.[59]

Even though the court did not find in Ms. Ehling's favor because her employer accessed the information through an unsolicited showing from one of her Facebook friends (i.e. someone with proper authorization to access the content),[60] the Court's finding shows that the SCA can be tailored and/or interpreted to protect private social media content through an analysis of the term "authorized." If an employee or applicant can prove that the action of handing over his or her login information was somehow coerced or was otherwise an involuntary act, then the employer could not claim authority as a defense to liability under the SCA.[61]

In the case of *Crispin v. Christian Audigier, Inc.*, the Court gave some clarification on the proper ways to use the SCA to protect against employer access to social media content.[62] While factually dissimilar to *Ehling* in a number of ways, the court in *Crispin* utilized much of the same reasoning in its determination.[63] In determining whether subpoenas requiring social media sites, including Facebook and MySpace, should hand over comments made by one of their users, the District Court for the Central District of California again found that social media sites of this nature qualify as electronic communications services providers under the

[57] *Id.* at *3.

[58] *Id.*

[59] *Id.* at *7.

[60] *Id.* at *9.

[61] *Blumenthal*, *Schumer*, *supra* note 4 (stating that "Requiring applicants to provide login credentials to secure social media websites and then using those credentials to access private information stored on those sites may be unduly coercive and therefore constitute unauthorized access.").

[62] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 981–82 (C.D. Cal. 2010).

[63] *Id.* at 982–89.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

SCA.[64] The court also found that private postings and messages on these sites constitute electronic communications that are stored for backup and archival purposes, thus allowing them to fall under the SCA's protection.[65] The subpoenas requesting these private messages were subsequently squashed.[66]

While the Supreme Court has yet to officially adopt the SCA as a protection against unwelcome employer access to private social media content, this case highlights the Act's potential. Not only does it show a judicial recognition of the need for privacy in certain types of social media content, but it also highlights the distinct qualities of social media that allow it to fall under the SCA's protection. Considerations of the SCA's relationship to social media are still developing, but based on the outcomes of these cases, it is not unreasonable to believe that courts may soon find the SCA provides protections that adequately address the concerns proposed password protection laws seek to remedy.

C. The National Labor Relations Act

Section 7 of the National Labor Relations Act ("NLRA") protects employees from adverse employment actions taken in response to engagement in "concerted activities" with other employees.[67] While the NLRA does not define concerted activity within the statute, the National Labor Relations Board ("NLRB") has stated that it considers concerted activity to be present when an employee acts with or on behalf of other employees, and not solely for himself or herself, for the purpose of discussing shared concerns about the terms and conditions of employment, even if no action is taken beyond that discussion.[68] The practical difficulty with this definition is that it is subject to interpretation and has not created a bright-line rule for determining when an employee's social media conduct has reached the level of protected concerted activity.[69] Section 8(a)(1) of the NLRA outlines potential liability for employers who violate Section 7's right to engage in concerted activity.[70]

---

[64] *Id.* at 982.

[65] *Id.* at 989.

[66] *Id.* at 991.

[67] National Labor Relations Act, 29 U.S.C. § 157 (2012).

[68] Robert Sprague, *Facebook Meets the NLRB: Employee Online Communications and Unfair Labor Practices*, 14 U. PA. J. BUS. L. 957, 960 (2012) (citing to Advice Memorandum from the NLRB Office of the Gen. Counsel to Cornele A. Overstreet, Regional Director of Region 28, Sagepoint Financial, Inc., No. 28-CA-23441, 2011 WL 3793672, at *2 (Aug. 9, 2011)).

[69] *Id.* at 994.

[70] 29 U.S.C. § 158 (2012).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

The NLRB's concern with employer utilization of employees' social media content is obvious; employer surveillance of social media conversations has the potential to chill employee speech and prevent employees from engaging in meaningful discussions related to their employment conditions.[71] This aversion to employer surveillance does not extend to situations where an employer claims that it learned information through another employee, much like the reasoning the court employed in the *Ehling* case mentioned above.[72] Additionally, the right to concerted activity cannot be claimed when the speech in question is merely a personal complaint regarding working conditions; there must be some sort of group activity involved.[73]

The NLRB considers it a violation of an employee's Section 7 rights when an employer's rules and actions are reasonably likely to prevent employees from engaging in their right to concerted activity.[74] A rule can either explicitly prohibit protected activity or it can implicitly prohibit protected activity if (1) employees would reasonably construe the language of the rule to prohibit Section 7 activities, (2) the rule was propagated in response to union activity, or (3) the rule has been applied to restrict the exercise of Section 7 rights.[75]

In the past few years, the NLRB has received over 100 complaints regarding employer action taken in conjunction with employee social media postings.[76] In a few circumstances, where a social media post involved the conditions of an employee's workplace and it garnered the attention and commentary of multiple employees, it was determined that adverse employment decisions were made in response to concerted activity on a social media site.[77] For example, the NLRB decided in favor of a terminated employee who took to Facebook to express her outrage at being demoted to a lower paying position within the collections agency where she worked.[78] Two co-workers plus several former co-workers posted messages of support alongside her complaint and expressed their similar sentiments

[71] Sprague, *supra* note 68, at 968.

[72] 18 U.S.C. § 2510(17).

[73] Sprague, *supra* note 68, at 973.

[74] *Id.* at 968.

[75] *Id.* at 968–69.

[76] *Id.* at 957.

[77] Memorandum from Lafe Solomon, Acting Gen. Counsel, NLRB to All Regional Directors, Officers-in-Charge, and Resident Officers, *Report of the Acting Gen. Counsel Concerning Social Media Cases*, at *2 (Jan. 24, 2012), *available at* http://mynlrb.nlrb.gov/link/document.aspx/09031d45807d6567.

[78] *Id.* at *5.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

about their employer.[79] The collective nature of this communication as well as its narrow content dealing solely with working conditions allowed this case to fall squarely within the protections of the NLRA.[80]

In most cases, however, the NLRB determined the employee speech at issue did not constitute protected concerted activity, as it either did not engage other employees (i.e. it constituted a personal gripe and not an invitation for discussion), or it was unrelated to working conditions as a whole.[81] For instance, the NLRB decided against an employee who was punished after posting a derogatory Facebook status about her employer during her lunch break.[82] While a few of her coworkers "liked" the status update, the NLRB held that this was insufficient to prove incitement of group discussion or action.[83]

These NLRB decisions, along with the many others that accompany them, show that while the NLRA is applicable to claims for employer misuse of private social media content, there is also an important functional limitation of its use; the protection provided is specific to the content of the speech at issue.[84] Only conversations that fall within the confines of the Act's narrow provisions will be granted protection.[85] Standing alone, therefore, the NLRA arguably provides minimal protection for those who wish to keep their social media content separate from their work lives.

D. The Fourth Amendment

Since the vast majority of cases involving an employer requesting an employee or job applicant's social media login information comes from employers in the public sphere,[86] a note on Fourth Amendment protections is warranted. The Fourth Amendment protects private citizens from unreasonable searches and seizures performed by government agents.[87] The Supreme Court has elaborated on the scope of the Fourth Amendment's protection, ruling the right against unreasonable searches and seizures still applies even when the affected individual

---

[79] *Id.*

[80] *Id.*

[81] *Id.* at *7.

[82] *Id.*

[83] *Id.*

[84] 29 U.S.C. § 157 (2012).

[85] *Id.*

[86] *See* Kauffman, *supra* note 16.

[87] U.S. CONST. amend. IV.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

is an employee of the government and the government agent is acting in its capacity as employer.[88] This protection is somewhat lessened in employment cases as opposed to criminal circumstances; in the employment context, the protection the Fourth Amendment provides is limited to the legitimate employer need of providing a safe, proficient working environment and does not include protections such as the warrant and probable cause requirements that would be available in a criminal prosecution.[89]

The scope of Fourth Amendment protection is governed primarily by the case of *Katz v. United States*, in which the Court determined the Amendment protects those who have a "reasonable expectation of privacy" in the area being searched.[90] The test for determining when such a reasonable expectation of privacy exists comes from Justice Harlan's concurrence in *Katz*, which requires a two-step inquiry.[91] First, the party seeking redress must prove he or she had a subjective expectation of privacy in the place being searched.[92] Once this has been proven, that party must also prove that he or she had an objective expectation of privacy that society would be willing to accept as reasonable.[93] Given the fact that this test does not create any bright-line test for a determination of reasonableness, courts are often required to use their discretion in analyzing what is "reasonable" conduct under society's modern expectations.[94]

In addition to *Katz*'s reasonableness requirements, the case of *O'Connor v. Ortega* outlines additional considerations to use when determining Fourth Amendment violations in the employment context.[95] Using the *O'Connor* test, the court looks to see if the employee had a reasonable expectation of privacy in the area being searched by the employer, following the framework established in *Katz*.[96] Once this requirement has been met, the court is then called upon to determine if the intrusion was reasonably justified, taking into consideration factors

---

[88] O'Connor v. Ortega, 480 U.S. 709, 714 (1987).

[89] Skinner v. Ry. Labor Executives' Assoc., 489 U.S. 602, 623 (1989).

[90] Katz v. United States, 389 U.S. 347, 353 (1967).

[91] *Id.* at 361 (Harlan, J., concurring).

[92] *Id.*

[93] *Id.*

[94] Alexander Naito, Comment, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. PA. J. CONST. L. 849, 860 (2012).

[95] O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

[96] *Id.* at 715.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

such as the extent and invasiveness of the intrusion and any legitimate government reasons behind the search.[97]

Keeping this framework in mind, the main issue that arises when utilizing the Fourth Amendment becomes proving that a person's expectation of privacy was reasonable under the circumstances.[98] Public social media content obviously does not meet this standard, but even information that has been placed under the strictest privacy settings can run into issues because of a theory called the Third Party Doctrine.[99] Under the Third Party Doctrine, a person cannot have a reasonable expectation of privacy in information that he or she voluntarily hands over to a third party, regardless of whether or not the information was handed over to that third party in confidence.[100] The definition of a "third party" can encompass just about any individual or organization.[101]

Under a strict reading of the Third Party Doctrine, the fact that a conversation was held over the Internet using the services of a social media platform such as Facebook or Twitter would disqualify such a conversation from Fourth Amendment protection.[102] Nevertheless, the Supreme Court has yet to decide a Fourth Amendment case related to employer intrusion into private social media content, and many scholars argue that public policy dictates a change in such a strict interpretation of the rule.[103] Therefore, while the Fourth Amendment is unlikely to provide much protection at the present time, the future of the Third Party Doctrine and its applicability to private social media content should not be considered set in stone.

---

[97] *Id.* at 719.

[98] *Katz*, 389 U.S. at 353.

[99] United States v. Miller, 425 U.S. 435, 443 (1976).

[100] *Id.*

[101] *Id.*

[102] Naito, *supra* note 94, at 868.

[103] *Id.* at 875; *see also* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2215–16 (2009).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

E. The Fair Credit Reporting Act

One common way employers vet potential employees is by requesting these employees' credit reports in order to determine their general reliability.[104] In order to ensure that such reports are compiled with a certain degree of accuracy, Congress passed the Fair Credit Reporting Act ("FCRA").[105] The FCRA applies to any "consumer report"[106] compiled by a "consumer reporting agency."[107] Given the relatively broad statutory definitions for both a consumer report and a consumer reporting agency, a social media background check of either public or private content performed by an outside agency would in most circumstances be subject to the standards of the FCRA.[108]

While it may provide relief in limited circumstances, it is important to note the main functional limitation of utilizing the FCRA in an action against an employer for invasion into private social media content; the FCRA only applies to third-party vetting of social media content.[109] The Act does not purport to regulate review of social media sites by internal members of an organization.[110] It is therefore easy for an employer to circumvent this protection by choosing to perform an unofficial review of social media content without the help of an established outside background-checking agency.[111]

Despite this major setback, utilization of the FCRA in cases involving intrusion into private social media content may not be completely devoid of value. Starting in 2010, some companies have begun utilizing third party vetting

---

[104] Nathan J. Ebnet, Note, *It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, 97 MINN. L. REV. 306, 312 (2012).

[105] Fair Credit Reporting Act, 15 U.S.C.§ 1681 (2012).

[106] 15 U.S.C. § 1681a(d)(1) (2012) (defines a "consumer report" as "Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's . . . character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for . . . employment purposes.").

[107] 15 U.S.C. § 1681(f) (2012) (defines a "consumer reporting agency" as any entity that "regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.").

[108] Ebnet, *supra* note 104, at 307.

[109] 15 U.S.C. § 1681 (2012).

[110] *Id.*

[111] Ebnet, *supra* note 104, at 308.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

companies that specialize in social media.[112] While the cost and logistical difficulties of utilizing a third party for social media background checks still weigh heavily on employers, the benefits of third party social media screening are slowly gaining traction.[113] These third party professionals remove any irrelevant information or evidence of a protected Title VII trait from their final reports, thereby significantly limiting an employer's risk of liability.[114] The FCRA's effectiveness in protecting private social media content will likely turn on the development of these third party agencies.

III. PRACTICAL DIFFICULTIES IN DRAFTING A SUFFICIENTLY TAILORED PASSWORD PRIVACY LAW

There are a number of practical issues that arise in the process of drafting password protection legislation. First, such legislation is inherently employee-friendly. Therefore, it is important to remember when drafting such laws they should not be so overly broad as to completely ignore legitimate business interests that employers may have, such as investigating harassment claims and avoiding liability for negligent hiring, especially in circumstances where the job in question requires a great deal of public trust.

Second, and related to the first issue, there is the question of what activity counts toward an employer coercing private information from an employee. While explicitly forcing an employee or applicant to provide login information for their social media accounts may seem like obvious coercion, other activities fall into a gray area. For example, is it coercive to request but not require an employee or applicant to provide an employer with login information? To "friend request" an employee or applicant on social media sites? To ask an employee or applicant to log in to his or her social media account in the presence of the employer? These questions can lead to ambiguity in the final draft of a password protection law, making it confusing for employers to understand their limitations and for employees and applicants to understand their rights.

A. Legitimate Business Interests

While intrusion into an employee's privacy is rarely a pleasant experience, it is oftentimes warranted due to legitimate business interests. Employers can have a

[112] *Id.*

[113] *See* SOCIAL INTELLIGENCE, http://www.socialintel.com (last visited Mar. 5, 2014).

[114] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

number of concerns that require greater intrusion into the social media lives of their employees or potential employees.

One such area of law that creates a possibility of liability is the doctrine of negligent hiring.[115] Liability for negligent hiring arises when an employee of an organization commits a tort, and it can be proven that the employer breached its duty to use reasonable care in determining that the employee was competent when it made the decision to hire him or her.[116] In this context, the "reasonable care" requirement warns that if a reasonable investigation would have uncovered an employee or potential employee's dangerous characteristics, then the employer faces liability.[117] Therefore, businesses have a legitimate interest in ensuring the people they hire and the employees they maintain do not possess any characteristics that would render them unfit for their position and dangerous to other people.[118]

Employers are well aware that the increase in social media usage amongst employees creates greater potential for workplace harassment.[119] Nowadays, not only can coworkers harass an employee within the confines of the business setting, they can also seek that employee out online.[120] Not only can this create an inefficient and hostile working environment, there is also the possibility of employer liability if the employer knew or reasonably should have known that harassment was taking place and did nothing to correct it.[121] Therefore, access to private social media content may be necessary in order to fully investigate claims of such behavior, to monitor inter-office communications for inappropriate statements, and to ensure that the employer is putting in a reasonable amount of care in seeking to prevent harassment disputes.[122]

Especially in the public sector, employers also have reason to be concerned about the dissemination of information gained as a result of an employment relationship.[123] While the result of leaked confidential information in the private

---

[115] Di Cosala v. Kay, 450 A.2d 508, 515 (N.J. 1982).

[116] *Id.*

[117] Mark Minuti, Note, *Employer Liability Under the Doctrine of Negligent Hiring: Suggested Methods for Avoiding the Hiring of Dangerous Employees*, 13 DEL. J. CORP. L. 501, 502 (1988).

[118] *Id.*

[119] Naito, *supra* note 94, at 862.

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

sector may result in monetary damages of varying degrees, confidential information in the public sector often covers issues of public welfare and safety.[124] Allowing employee access to this type of information carries with it an obvious burden to ensure that such information does not become a societal detriment, and thus it is imperative that it not be released to the general public, either through a public social media posting or a private message to a friend.[125] The legitimacy and persuasiveness of this business interest will therefore depend on the job at issue in each case, but it remains a genuine concern in all employment situations where confidential information may be present.

B. What Provisions Should Be Included?

The disparities in protections provided by the various state laws now in place, or being considered, demonstrate how many considerations need to take place when determining the appropriate provisions to include in a well-drafted law. For instance, some laws only outlaw requesting or requiring passwords for personal social media accounts,[126] whereas others go further and prohibit employers from viewing password-protected material in the presence of the employee or applicant.[127] These differences can create confusion for employers as far as what they are and are not allowed to do, opening them up to liability should they fail to adequately research the laws of the various states in which they conduct business.

The wording of the statute is also important. Some statutes go so far as to prohibit employers from "demanding access in any manner" to an employee or applicant's private social media content, raising the question of whether or not a friend request from a supervisor would be appropriate under a strict reading of the statute.[128] Others are arguably less restrictive, prohibiting an employer from requesting that it be "allowed observation of" private social media content, but still raise the issue of statutory ambiguity.[129] Again, ambiguity in statutory language can create confusion amongst employers who wish to utilize social media checks to the

[124] *Id.*

[125] Naito, *supra* note 94, at 862.

[126] *See* 820 ILL. COMP. STAT. 55/10 (2013); *see also* MD. CODE ANN., Lab. & Empl. 3-712 (West 2013).

[127] *See* CAL. LAB. CODE § 980 (2012); *see also* DEL. CODE ANN. tit. 14, § 8102 (2012).

[128] Assemb. B. 2879, 215th Leg. (N.J. 2012), *available at* http://www.njleg.state.nj.us/2012/Bills/A3000/2879_I1.HTM.

[129] Internet Privacy Protection Act, H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012), *available at* https://www.legislature.mi.gov/documents/2011-2012/publicact/pdf/2012-PA-0478.pdf.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu

fullest extent allowable under the law, raising the risk of liability should these employers fail to interpret such language correctly.

IV. CONCLUSION

While password protection legislation is not necessarily a detriment to the employment landscape, the current rush towards legislation is based on inadequate information as to the prevalence of questionable behavior and a less than thorough analysis of the protections that are already in place. By allowing our understanding of social media use in employment settings to develop further, we cut the risk of poorly drafted legislation that creates undue burdens on businesses, confuses affected parties, and wastes legislators' time and efforts. Hesitancy and a healthy amount of skepticism towards such laws will ensure that should sufficient evidence arise dictating a need for protections, the legislation that comes forth will be well informed, well-reasoned, and tailored to the issues at hand.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.142 ● http://tlp.law.pitt.edu