5-1-2013

Privacy Rights in the Age of Social Media: Facebook Passwords and Legal Implications

Marlene Botros

Privacy Rights in the Age of Social Media: Facebook Passwords and Legal Implications

Marlene Botros

TABLE OF CONTENTS

INTRODUCTION: FACEBOOK IN THE MODERN WORLD

Social media in modern society serves a wide array of functions in daily life. Social networking sites such as Facebook are powerful tools that can reveal information and act as a means of communication that is unprecedented in the digital age. However, it is easy to see how these sites can be misused. Particularly, employers are eager to obtain information located on Facebook in order to discern the true identity of their employees or potential employees.

Facebook is a social media site that is primarily a means of communication, allowing individuals to create personal profiles, and navigate the profiles of other users who grant them access to some or all of their uploaded information.[1] Facebook, which now has over one billion users[2], may contain intimate details of a user's self-identity. These profiles can include information concerning anything from a user's relationship status and political affiliations to photos and status updates from where the user was last Friday evening. A recent hiring trend has proven that certain employers have no qualms about taking the leap and requesting a Facebook password as a prerequisite to hiring an employee.[3] This paper will address the current and ambiguous state of the law on this subject, as well as the potential future of employers' rights to obtain the valuable and personal information of employees' Facebook passwords.

---

[1] See Facebook, http://www.facebook.com/ (last visited December 9, 2012).

[2] Fact Sheet, Facebook, http://newsroom.fb.com/News/457/One-Billion-People-on-Facebook ("[m]ore than one billion people using Facebook actively each month.") (last visited December 2, 2012).

[3] Protecting Your Passwords and Your Privacy, Facebook, http://www.facebook.com/note.php?note_id=326598317390057 ("([a] distressing increase in reports of employers and others seeking to gain inappropriate access to people's Facebook profiles or private information.") (last visited November 5, 2012); Michelle Singletarry, "Would You Give Potential Employers Your Facebook Password?" *Wash. Post*, Mar. 29, 2012 http://www.washingtonpost.com/business/economy/would-you-give-potential-employers-your-facebook-password/2012/03/29/gIQAlJiqiS_story.html (last visited December 5, 2012).

THE ISSUE: PRIVACY AND THE WORKFORCE

It is evident that employers want to ensure they have the right person for the job before committing to hire. However, the lines are blurred in determining when employers overstep their boundaries when assessing job candidates. Traditionally, a resume, cover letter, and list of references are provided to potential employers to demonstrate a job candidate's character, in addition to their merits and experiences.[4] Yet, as digital media increasingly becomes a part of everyday life, it seems that employers are finding creative and more intrusive methods to discover information that may not be readily divulged in a traditional interview process.[5]

A. EMPLOYER'S INCENTIVE TO OBTAIN FACEBOOK PASSWORDS

It is arguable that Facebook profiles hold the very essence of a person's character; a person's interests as well as likes, dislikes, and personality may be reflected in a user's profile. Separate from the privacy issues at hand, employers have a strong business incentive to discover all they can about a job applicant before committing to hiring them. From the employer's perspective the repercussions of making a bad hiring decision may prove to cause irreparable harm for an employer's business. Gaining additional insight into a person's character, which can take a little too long to discover without accessing the ready information on Facebook, can prevent such a situation from ever taking place.

With no explicit federal law stating anything to the contrary, it is no wonder that many employers have made a bold leap in requesting Facebook passwords from their employees and

---

[4] Alissa Del Riego, Patricia Sánchez Abril, Avner Levin, *Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy*, 16 NO. 3 J. Internet L. 1, 23 (2012).
[5] *Id.* at 17.

potential hires. In the absence of Federal law, employees and applicants may have a tough decision to make: their job, or their privacy.

B. FACEBOOK'S REACTION: STATEMENT OF RIGHTS AND RESPONSIBILITIES

Facebook's Chief Privacy Officer, Erin Egan, recently disclosed an official statement entitled "Protecting Your Passwords and Your Privacy".[6] The statement implores users to keep their passwords private, as by doing otherwise would violate Facebook's Statement of Rights and Responsibilities. It makes clear that you should never have to reveal your Facebook passwords to anyone, which includes prospective employers. She claims that Facebook has worked very hard to ensure everyone has the necessary tools to keep their information private. Sharing your password would not only violate your privacy, but also the privacy of your friends and loved ones who have shared information with you through Facebook's social networking.[7]

The statement goes on to say that by requesting such private information, employers may open themselves up to liability.[8] For example, since Facebook stores such information as political and religious affiliations, national origin and other demographics constituting protected classes, if the employer discovers this information and later does not hire that person, they could be subject to liability. It is evident that these employment practices are a clear violation of Facebook's Terms of Service. Beyond that however, is a nebulous tangle of federal laws that do not establish clear legal outcomes of such behavior.

---

[6] *Protecting Your Passwords and Your Privacy*, *Facebook*, http://www.facebook.com/note.php?note_id=326598317390057 (last visited December 9, 2012).

[7] *Id.* ("[a]s the friend of the 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' intent to share with just because that user is looking for a job.").

[8] *Id.* ("[i]f an employer sees on Facebook that someone is a member of a protected group (e.g. over a certain age, etc.) that employer may open themselves to claims of discrimination if they don't hire that person.").

C. FACEBOOK'S TERMS OF SERVICE

Facebook's "Terms of Service" is an agreement that each user enters into with Facebook when creating their online Facebook account.[9] This agreement specifically states that the user owns all the content and information posted on their Facebook profile.[10] The user has full control over how that content is shared through Facebook's privacy and application settings. Further, Facebook makes it the user's responsibility not to solicit any login information or request access to an account that belongs to someone else. The agreement also stresses that by joining Facebook you cannot use it as a means to do anything unlawful, misleading, malicious or discriminatory.[11]

If a user violates the Terms of Service there is little recourse through Facebook. The agreement states that if the user violates these Terms of Service, Facebook will stop providing all or part of Facebook's services to the user.[12] Unfortunately, this reprimand means little to an applicant or employee against who suffered as a result of the violation of this agreement. Furthermore, by definition, this agreement only applies if you are a user of Facebook. In that case, if the employer asking for a potential employee or employee's login information does not use Facebook, none of these terms apply to them, leaving victims of the violation with no existent remedy through Facebook.[13]

CURRENT LAW

There are two federal statutes that may give employees a cause of action against employers who ask for Facebook passwords, the Stored Communications Act and the Computer

[9] Facebook: Statement of Rights and Responsibilities, http://www.facebook.com/legal/terms (last visited December 2, 2012).
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*

Fraud and Abuse Act. As discussed below, there are many difficulties that could arise if a plaintiff attempts to bring a private right of action through these statutes. Beyond these two statutes, damaged employees may seek indemnities through torts claims, contract law, certain labor laws as well as Title VII discrimination claims.[14]

A. STORED COMMUNICATIONS ACT

The purpose of the Stored Communications Act (SCA) is to prohibit intentional access to electronic information without authorization. Enacted in 1986 as an extension of the fourth amendment of the constitution, this act penalizes anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided or… intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."[15] In addition to criminal penalties, a plaintiff may recover civil damages under the SCA.[16] While there is no particular fixed point at which nominal damages become actual damages, plaintiffs have to show that they have suffered some form of concrete, compensable harm as a result of the defendant's alleged SCA violations.[17]

The law makes exceptions in a few cases, two of which are relevant in this analysis. First, if the person or entity providing a wire or electronic communications service authorized the conduct, then there is no offense.[18] Second, this law does not prohibit conduct that was

---

[14] Alissa Del Riego, Patricia Sánchez Abril, Avner Levin, *Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy,* 16 NO. 3 J. Internet L. 1, 23 (2012).

[15] Stored Communications Act, 18 U.S.C. §2701.

[16] 18 U.S.C. §2707(c) ("The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000").

[17] 18 U.S.C. §2707(c), See *Global Policy Partners, LLC v. Yessin*, 686 F. Supp. 2d 642 (E.D. Va. 2010).

[18] Stored Communications Act, 18 U.S.C. §2701(c)(1).

authorized by a user of that service with respect to a communication of or intended for that user.[19] The purpose of Congress enacting the SCA is to "protect privacy interests in personal and proprietary information from the mounting threat of computer hackers 'deliberately gaining access to, and sometimes tampering with, electronic or wire communications' by means of electronic trespass."[20]

The main issue in analyzing the concern of employer solicitation of Facebook passwords under the SCA is that the law does not apply easily to social networking websites. These websites do not fit in to any categories that are detailed in the statute.[21] Thus, many difficulties arise when analyzing this law in regards to employers asking employees for their Facebook passwords. First, the law only prohibits intentional access without authorization to a facility through which electronic communications service is provided.[22] In order to have protection under this law, it must be determined that Facebook constitutes a facility through which electronic communications service is provided. According to the 9th Circuit, "[t]he Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents…the Act protects users whose electronic communications are in electronic storage with an ISP [Internet Service Provider] or other electronic communications facility."[23]

Under the definitions chapter of the SCA, the law provides that an electronic communications system is defined as "any wire, radio, electromagnetic, photooptical or

---

[19] Stored Communications Act, 18 U.S.C. §2701(c)(2).

[20] *Maremont v. Susan Fredman Design Group, Ltd.*, 2011 WL 6101949 (N.D. Ill. Dec. 7, 2011).

[21] Lindsay S. Feuer, Who Is Poking Around Your Facebook Profile?: The Need to Reform the Stored Communications Act to Reflect A Lack of Privacy on Social Networking Websites, 40 Hofstra L. Rev. 473, 496 (2011).

[22] Stored Communications Act, 18 U.S.C. §2701(a)(1).

[23] Theofel v. Farey-Jones, 359 F.3d 1066, 1072-73 (9th Cir. 2004).

photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[24] Furthermore, an electronic communication service means "any service, which provides to users thereof the ability to send or receive wire or electronic communications."[25]

In *Crispen v. Christian Audigier, Inc.*, private messaging and email services provided by social networking websites and web hosting sites constituted "electronic communication services" (ECS) under the SCA.[26] The court reasoned that these websites provide services, such as posting messages on an account holder's "wall" and allowing users to leave comments on another account holder's web page, all of which account holders could limit access to. However, the SCA's definition of ECS does not extend to a completely public bulletin board system. This means that if a user has a completely public profile that an employer can access, this would merit no protection under the SCA.[27]

Even if Facebook does constitute a facility through which an electronic communications service is provided, the intentional access to this information needs to be "without authorization" for employers to be liable under the SCA. Thus, as is the case when employers ask for Facebook passwords, the Facebook user will have consented to such access by conceding to hand over the password. If the conduct was authorized, the access would fall under the second exception to the SCA and no liability would attach. Recent case law has shed light on what constitutes authorized access regarding employee social media accounts.

---

[24] 18 U.S.C. §2510(14).
[25] 18 U.S.C. § 2510(15).
[26] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).
[27] *Id.* at 980.

Pietrylo v. Hillstrone Restaurant Group is a particularly illuminating case.[28] At issue was whether an employee, who voluntarily gave access to a private social media group to the employer, constituted authorization under the statute. The employees had created a private group on the social media site MySpace, and used it to discuss their work at the restaurant. In this electronic discussion, the employees made many negative comments regarding management and their work environment. This was a private group that could only be accessed by invitation. When the restaurant management became aware of the group, they asked an employee for access. The employee provided access to management. Subsequently, two employees were terminated because of their critical comments in the MySpace group. Although the employee who provided access testified that she did not feel coerced, she felt compelled to provide access simply because they were management and she did not want any adverse employment actions to be taken against her.[29]

The employees sued over what they perceived as wrongful termination, alleging that the management's behavior was a violation of the Stored Communications Act as well as the corresponding New Jersey Statute. The employers argued that the employee was an authorized user, who provided access to the employers, so there can be no liability based on the statute's exception. The New Jersey District Court held that summary judgment could not be authorized in this case because there is a material dispute regarding whether her consent was voluntarily given. The court further reasoned that if her consent was given under duress, then management was not authorized under the terms of the statute.[30]

---

[28] *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009).
[29] *Id.* at 3.
[30] *Id.*

In analyzing what the term "authorized" means, the court cites the 9th Circuit case, *Konop v. Hawaiin Airlines, Inc*.[31] There, an employer gained access to an employee's secure website through a third party who was granted access, but was not considered a user under the statute's definition. Although "§ 2701(c)(2) of the SCA 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 intended for that user,"' the Ninth Circuit reasoned that a non-"user" cannot grant access to a third party under the SCA."[32] The court held that an employer is liable for coercing access to a social media website, and even though it was through more indirect means, that conduct constituted access without authorization to "a facility through which an electronic communication service is provided." Stated another way, even though the employee was authorized to use Konop's website, the employee never actually logged on to and used the website. Thus, he was not considered a "user" of the site. Since one must first be a "user" to satisfy the first prong of the § 2701(c)(2) SCA liability exception, the employee does not qualify and therefore could not grant access to the vice president without violating the SCA.[33]

These cases show that bringing a claim under the SCA for an employer's request of a Facebook password is possible, though it is fact sensitive. If the plaintiff can demonstrate that their Facebook account is a facility through which an electronic communication service is provided, that is only half the battle. It remains to be shown by the plaintiff that the login access was provided under duress or coercion and was thus not authorized by the employee. Only then is it is possible for a terminated employee or a qualified applicant to successfully bring a claim under the Stored Communications Act.

---

[31] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002).

[32] Catherine Crane, *Social Networking v. the Employment-at-Will Doctrine: A Potential Defense for Employees Fired for Facebooking, Terminated for Twittering, Booted for Blogging, and Sacked for Social Networking*, 89 Wash. U.L. Rev. 639, 672 (2012).

[33] *Id.*

B. COMPUTER FRAUD AND ABUSE ACT

Similar to the Stored Communications Act, the Computer Fraud and Abuse Act (CFAA) makes it a criminal offense to knowingly or intentionally access a computer without authorization in order to obtain information.[34] Under this statute, an employee can seek both civil and criminal penalties, money damages, and injunctions against their current or future employer.[35] The relevant part of the statute reads as follows: "Whoever—intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains... information from any protected computer…" shall be punished in accordance with subsection (c) of this section.[36] In addition, to successfully bring a claim under the CFAA, the damage caused by the defendant must be more than $5,000 in a one-year period.[37]

The CFAA does not require intent to defraud or that the defendant knew the value of the information obtained.[38] Rather, the crime of accessing a protected computer without authorization and obtaining information from that computer only requires proof that the defendant intentionally accessed information from a protected computer.[39] Furthermore, although it is in the name of the statute, "fraud" under the Computer Fraud and Abuse Act only requires a showing of unlawful access. There is no need to plead the elements of common law fraud to state a claim under the Act.[40]

---

[34] 18 U.S.C. §1030.
[35] 18 U.S.C. §1030(g), see Shawn E. Tuma, "*What Does Cfaa Mean and Why Should I Care?"-A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. Rev. 141, 158 (2011).
[36] 18 U.S.C. §1030.
[37] 18 U.S.C. §1030(a)(4).
[38] *United States v. Willis*, 476 F.3d 1121, 1124 (10th Cir.2007).
[39] *Id.* at 1124.
[40] *eBay Inc. v. Digital Point Solutions, Inc.*, 608 F.Supp.2d 1156, 1164 n. 6 (N.D.Cal.2009).

Employees who provide their Facebook passwords to employers will have greater difficulty bringing a private right of action under the CFAA than the SCA. In order to successfully bring a claim under the CFAA, an employee or applicant would have to show that an employer intentionally accessed their Facebook page, or other social media site, without authorization, or exceeded such authorization, in order to obtain information from a protected computer. As a result of this unlawful behavior, the plaintiff must also show they suffered a damage of over $5,000 in less than a one-year period.[41]

Similar to the SCA, a portion of CFAA liability hangs on whether the defendant was authorized in accessing the employee's Facebook page or any other social media website. The statute does not define what constitutes "access" or "authorization" and thus, courts have been free to interpret these terms.[42] A violation for accessing information "without authorization" under the CFAA occurs only where initial access is not permitted.[43] The 9th Circuit has held that it is a "fundamental canon of statutory construction ... that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning." Thus, authorization was construed as permission, because the dictionary defines authorization as "permission or power granted by an authority".[44] In *United States v. Morris*, the 2nd Circuit held that for the purposes of the CFAA, the word "authorization" is of common usage, and "without any technical or ambiguous meaning," Accordingly, the district court was not obliged to instruct the jury on it's meaning.[45] Courts have characteristically examined the extent of a user's authorization to

---

[41] 18 U.S.C. §1030(a)(4).

[42] Andrew T. Hernacki, *A Vague Law in A Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 Am. U. L. Rev. 1543, 1555 (2012).

[43] 18 U.S.C. §1030.

[44] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009).

[45] *United States v. Morris*, 928 F.2d 504, 511 (2d Cir.1991).

access a computer on the basis of the expected standards of intended use, as well as analyzed the type of relationship established between the computer's owner and the user.[46]

In *United States v. Drew*, a California district court assessed whether violations of a website's Terms of Service, specifically MySpace, violated the CFAA.[47] The defendant, Lori Drew, was charged with cyber bullying, a misdemeanor under the statute, of a thirteen year old girl who subsequently committed suicide. The court analyzed the meaning of the term "unauthorized access" to determine if Drew's conduct violated the statute. The government argued that Drew's conduct was unauthorized, when she created a profile under the false alias "Josh Evans", a violation of the MySpace Terms of Service. The question then turned on whether basing a CFAA misdemeanor violation on the conscious violation of MySpace's Terms of Service would invalidate the statute as a result of the void-for-vagueness doctrine. The court held that Drew's conduct did not violate the CFAA, and found that allowing a violation of the CFAA on the basis of a violation of a website's Terms of Service would transform the CFAA into "an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals."[48]

The analysis under Drew would not bode well for employees and applicants, who hope to bring a claim under the CFAA for a violation of Facebook's Terms of Service by their employer. Furthermore, a violation for "exceeding authorized access" would not assist those who fall victim of social networking snooping. Under the CFAA, exceeding authorized access occurs where initial access is permitted but the access of certain information is not permitted.[49] In the context of employee Facebook passwords, the clause "or exceeds authorized access" means that

---

[46] *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir.), cert. denied, 552 U.S. 820, 128 S.Ct. 119, 169 L.Ed.2d 27 (2007).
[47] *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009).
[48] *Id.* at 466.
[49] *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008).

even if employers were given authority to access employee's social media pages and they exceed the scope of that authority, the will be penalized for that behavior. However, Courts have been reluctant to construe this clause broadly.[50] In *AtPac, Inc. v. Aptitude Solutions, Inc.*, the court held that the county and its clerk recorder did not exceed their authorized access to a software developer's information on the county server.[51] The software developer only gave the county permission to access its directories and source code to shut down the server in the event of an emergency. However, when county employees accessed the developer's directories on the county server, it was in order to provide the developer's competitor with passwords and source code stored on the server. The court reasoned that the terms "exceeds authorized access simply examines whether the accessor was entitled to access the information for any reason. Rather, "trafficking" of passwords only becomes illegal when someone does so knowingly and with the intent to defraud, and by doing so the password enables the recipient to access the protected computer without authorization."[52]

Moreover, the CFAA is slightly less comprehensive than the SCA. In order to bring a civil claim under the CFAA, a plaintiff must prove that the loss or damage the defendant caused is more than $5,000 in any one year period.[53] The law states: "Whoever--knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, *unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period*".[54] This language adds

[50] See *AtPac, Inc. v. Aptitude Solutions, Inc., 730 F.Supp.2d 1174 (E.D.Cal.2010).*
[51] *Id.* at 1184.
[52] *Id.*
[53] 18 U.S.C. §1030(a)(4).
[54] *Id.* (Emphasis added)

additional obstacles for plaintiffs seeking relief under the CFAA. According to the CFAA, "loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[55]

Many cases have dealt with the question of what constitutes loss or damage under the statute. In *U.S. v. Middleton*, the court held that the CFAA, which makes it "an offense to cause damage to a protected computer, by knowingly causing the transmission of a program, information, code, or command, resulting in a specified loss to one or more 'individuals,' encompasses damage sustained by a business entity as well as by a natural person." [56] Furthermore, in *In re Doubleclick Inc.*, the court held that economic loss under the statute could not be established solely by sheer collection of data or information.[57] In terms of employer access to employee's Facebook passwords, loss or damages would most likely be adverse employment actions, such as demotion or termination. However, this would be a consequential damage under the CFAA. According to Illinois District Court, solely economic damages, which are unrelated to the computer systems, are not covered under the definition of "loss" in the CFAA.[58]

Moreover, in *Eagle v. Morgan, Et al.*, Eagle set up a LinkedIn account and gave an employee the login information.[59] When Eagle was terminated, the company assumed ownership and changed the information listed in the LinkedIn account to that of the incoming CEO, but

---

[55] 18 U.S.C. §1030(e)(11).
[56] *United States v. Middleton*, 35 F.Supp.2d 1189, 1192 (N.D.Cal.1999).
[57] *In re Doubleclick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001).
[58] *SKF USA, Inc. v. Bjerkness*, No. 08 C 4709, 2009 WL 1108494 (N.D.Ill. Apr.24, 2009).
[59] *Eagle v. Morgan*, 2011 WL 6739448 (E.D. Pa., Dec. 22 2011).

kept all of Eagle's achievements and awards. Eagle claimed this was a violation of the CFAA. The Court held that the potential loss of future business is insufficient. In addition, a loss to a person's reputation and/or relationship with clients does not arise to the level of a violation under the CFAA. Thus, the District Court dismissed Eagle's CFAA claim, and found that a loss of business opportunity caused by lack of access and control of Eagle's LinkedIn account failed to establish a CFAA violation. In addition, Eagle was not claiming an economic loss due to computer inoperability or that money was spent to repair any damages made to it. These cases illustrate how difficult it is for employees to successfully seek civil damages under the Computer Fraud and Abuse Act.[60]

POTENTIAL BACKFIRING: DISCRIMINATION SUITS

Employers may have a business incentive to use social media in the hiring process, both as a screening device as well as a means to ensure good character. According to the Society for Human Resourcing Management (SHRM), roughly 56% of employers responding to a survey stated that they use social media as part of the hiring process.[61] However, this use of social media could potentially backfire on the employer. Social media websites reveal particularly sensitive information about a person in the eyes of the law. Users often report their age, religious affiliations, disabilities and other protected class information when creating their online profiles.[62]

Aside from potential liability stemming from the SCA or CFAA, employers who insist on accessing potential employee's Facebook information run the risk of continuous employment

---

[60] *Id.*

[61] Scott Brutocao, *Issue Spotting: The Multitude of Ways Social Media Impacts Employment Law and Litigation*, 60 The Advoc. (Texas) 8 (2012).

[62] *Id.*

discrimination suits, which could be debilitating for some businesses.[63] Title VII discrimination claims, The Age Discrimination in Employment Act, and the Americans with Disabilities Act, are all examples of potential channels through which employees and applicants can bring private rights of action against their employers.[64] The case against the employer would be more robust if an applicant was not hired, or worse, fired, after the employer asked for their login information and discovered information placing them in a protected class.[65]

Specifically, in *Gaskell v. University of Kentucky*, the university was searching for a new director for an observatory.[66] The university search committee conducted an Internet search on the applicants, and discovered that Gaskell wrote a paper regarding the Bible and astronomy. Convinced that Gaskell wrote this paper in furtherance of his religious views on creationism, Gaskell was not hired. This was evidenced by an email from a search committee member stating that the "real reason" Gaskell was not hired was his religious beliefs. Gaskell sued, alleging religious discrimination, and the university sought summary judgment. The court held that summary judgment was not proper, because the search committee member's conduct created an issue of fact. Although it was settled, this case exemplifies the dangers faced by employers when they use social media as a tool in the hiring process.[67]

---

[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*, See *Gaskell v. Univ. of Kentucky*, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010).
[67] *Id.*

EMERGING LAW: A LEGAL ANALYSIS

A. EMERGING FEDERAL LAW

Although it may be difficult to find relief under the current state of the law, a few congressmen have been pushing for bills that would explicitly rectify this issue.[68] Recently, New York Congressman, Eliot Engel, proposed a federal bill entitled the Social Networking Online Protection Act (SNOPA).[69] This bill would "prohibit employers and certain other entities from requiring or requesting that employees and certain other individuals provide a user name, password, or other means for accessing a personal account on any social networking website."[70] Furthermore, the new law would prohibit any employer from discharging, discriminating against, disciplining, or denying employment or promotion to any employee or applicant who refuses to provide their account information, as well as any employee who has filed a complaint or proceeding relating to this title. Under this new law, a "social networking site" would mean any Internet service, platform, or website that provides a user with a distinct account-- (A) whereby the user can access such account by way of a distinct user name, password, or other means distinct for that user; and (B) that is primarily intended for the user to upload, store, and manage user-generated personal content on the service, platform, or website. This definition is quite broad; not only would this include Facebook and other social media sites, but e-mail pages, financial statements, and any other site requiring specific login information that contains personal content.[71]

---

[68] See Govtrack.us, http://www.govtrack.us/congress/bills/112/hr5050, http://www.govtrack.us/congress/bills/112/hr5684.
[69] *Id.*
[70] *Id.*
[71] Bill Text, Govtrack.us, http://www.govtrack.us/congress/bills/112/hr5050/text.

Instead of criminal penalties, this bill would impose civil penalties on employers who violate the act, including injunctive relief.[72] These civil penalties cannot exceed $10,000. In determining this amount, the previous compliance record with the new law, as well as the gravity of the violation will be taken into account. The injunctive relief under this chapter stretches from temporary restraining orders to employment reinstatement, promotion, and payment of lost wages and benefits.[73] This legislation would not only cover employers, but schools as well, to ensure that students would not have their privacy rights violated when applying to colleges and other institutions.[74]

However, it is uncertain how the chips will fall when Congress puts SNOPA to a vote. This would not be Congress's first attempt to pass bills regulating these business practices.[75] In March of 2012, the House of Representatives voted against a bill amending the Federal Communications Commission (FCC) Reform Act, which would have given the FCC the power to regulate social network privacy for employees.[76] This bill, proposed by Representative Ed Perlmutter of Colorado, would have made it unlawful to demand, as a condition of employment, that an employee or potential employee reveal their confidential password to any social media website. The bill was voted down 236 to 184, with only one republican voting in support of the bill, and only two democrats voting against the bill.[77] Republicans did note, however, that while they believed this proposed legislation would not change the current situation, they are willing to

---

[72] *Id.* at §2(b)(1).

[73] *Id.* at §2(b)(2) ("In any action brought under this section, the district courts of the United States shall have jurisdiction, for cause shown, to issue temporary or permanent restraining orders and injunctions to require compliance with this Act, including such legal or equitable relief incident thereto as may be appropriate, including, employment, reinstatement, promotion, and the payment of lost wages and benefits.").

[74] *Id.* at §9537, Prohibition on Access to Personal Accounts of Students.

[75] House Votes Down Plan to Block Employers From Facebook Snooping, cbsnews.com, http://www.cbsnews.com/8301-501465_162-57406472-501465/house-votes-down-plan-to-block-employers-from-facebook-snooping/ (last visited December 5, 2012).

[76] *Id.*

[77] See clerk.house.gov, http://clerk.house.gov/evs/2012/roll137.xml (last visited December 2, 2012).

work on an agreeable piece of legislation in the future, most likely one that does not provide the FCC with more regulatory power.[78]

SNOPA is not the only bill of this nature that has been introduced to Congress. Most recently, in May of 2012, Representative Martin Heinrich of New Mexico introduced the Password Protection Act of 2012 (PPA).[79] Similar to SNOPA, the PPA would prevent and prohibit employers from coercing any person to authorize access to a protected computer. Instead of criminal charges like the CFAA and the SCA, the new bill would only impose financial penalties on employers who violate the law. The PPA mirrors existing federal law, and is similar in scope to anti-hacking statutes, such as the Computer Fraud and Abuse Act. The text of the amendment would state that the prohibited activity includes:

> "[a]cting as an employer, knowingly and intentionally-- '(A) for the purposes of employing, promoting, or terminating employment, compels or coerces 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; or '(B) discharges, disciplines, discriminates against in any manner, or threatens to take any such action against, any person-- '(i) for failing to authorize access described in subparagraph (A) to a protected computer that is not the employer's protected computer; or '(ii) who has filed any complaint or instituted or caused to be instituted any proceeding under or related to this paragraph, or has testified or is about to testify in any such proceeding;'".[80]

In certain ways, the PPA is broad in scope than SNOPA. Not only does the statute extend to social networks, but it also encompasses all information stored on a computer that an employer attempts to coerce from an employee, and which does not belong to or is not in the control of the

---

[78] Sarah Jacobsson Purewal, "Facebook Password Amendment Rejected by Congress," PCWorld, Mar. 29, 2012, http://www.pcworld.com/article/252837/facebook_password_amendment_rejected_by_congress.html. ("Republicans argued that while the proposed legislation wouldn't help the situation, they were willing to work on new legislation in the future.")

[79] Govtrack.us, http://www.govtrack.us/congress/bills/112/hr5684.

[80] Bill Text, Govtrack.us, http://www.govtrack.us/congress/bills/112/hr5684/text.

employer.[81] The PPA focuses on the servers where the information is ultimately stored, instead of identifying types of Internet services, such as Facebook and other social media websites. By doing this, the new law would be "technology neutral", and thus would update as technology updates.[82]

However, the PPA is narrower in scope in other ways. Unlike SNOPA, this federal statute would not extend to students. Furthermore, this statute provides a few exceptions.[83] First, the statute provides an exemption for government employees who work with children under the age of thirteen.[84] Second, the statute allows the executive branch to wholly exempt specific classes of workers that come into contact with classified information, including soldiers. The law also preserves several employer rights, such as permitting social networking in the office on a voluntary basis and holding employees accountable for stealing data from their employers. Furthermore, the bill would allow employers to set their own policies for employer operated systems and accounts.[85]

Unfortunately, it is unlikely that SNOPA or the PPA will be passed into law. Last year, only 4% of all bills proposed to the House of Representatives were enacted.[86] Secondly, Congressman Eliot Engel as well as Congressman Martin Heinrich are members of the minority party, and there is a clear partisan split on this issue.[87] Although a similar bill may be passed in

---

[81] *Id.*
[82] *Id.*
[83] *Id.* at §2(d).
[84] *Id.* at §2(d)(2)(b)(ii) (a State enacts a law that specifically waives subsection (a)(8) with respect to a particular class of State government employees or employees who work with individuals under 13 years of age, and the employer's action relates to an employee in such class).
[85] *Id.* at §2(d)(2)(b)(i-iii).
[86] See http://www.govtrack.us/congress/bills/112/hr5050, http://www.govtrack.us/congress/bills/112/hr5684 (last visited December 2, 2012).
[87] *Id.*

the future, it seems unlikely that these particular bills will make it through the hurdles of being enacted.

B. EMERGING STATE LAW

Due to the ambiguity of current federal law, Maryland and Illinois have recently started a trend and have signed into law pieces of legislation that ban employers from requesting employee Facebook passwords.[88] Although Maryland and Illinois are among the first two, several other states have added, or are considering bans, including Washington, Delaware, California, and New Jersey. In fact, lawmakers in 10 other states have introduced legislation to limit what an employer can do with social media website usernames and passwords.[89] However, the lack of uniformity and overly broad language of these state laws may make it too difficult for employers to do their jobs properly.

1. MARYLAND

The state of Maryland was the first to pass legislation that bans employers from requesting employee passwords for social media websites.[90] The bill, entitled the User Name and Password Privacy Protection Act, states that this type of behavior violates privacy, as well as coerces employees and prospective employees.[91] Specifically, the law prohibits all Maryland businesses from requiring, or even asking, that applicants or employees disclose their user names or passwords for "any personal account or service" accessed through "computers, telephones,

---

[88] Scott Brutocao, *Issue Spotting: The Multitude of Ways Social Media Impacts Employment Law and Litigation*, 60 The Advoc. (Texas) 8, 10 (2012).
[89] *Id.* at 10.
[90] Senate Bill 433, http://mlis.state.md.us/2012rs/bills/sb/sb0433t.pdf (last visited December 2, 2012).
[91] *Id.*

personal digital assistants, and other similar devices."[92] However, the law does not authorize applicants or employees to sue employers who violate the act. Instead, employees who are terminated may have a claim for wrongful discharge in violation of public policy.[93]

Although this state law may seem broad, the law also makes expressly clear what it does not prohibit. First, the law does not prohibit employers requesting login access for "accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems."[94] This means that employees cannot rely on this law to stop employers from gaining access the employees store on the employer's own information systems. Secondly, the law does not prohibit an employer from conducting an investigation to make certain that the employee is complying with "securities or financial law, or regulatory requirements, when the employee is using an online account for business purposes." [95] Thirdly, employers can conduct an investigation in order to protect trade secrets if the employer receives information that an employee has downloaded proprietary employer information to their personal online account.[96] Fourthly, while the law prohibits employers from requesting to access "any personal account or service", the law does not prevent employers from requesting access to the employee's personal device, such as a smart phone.[97] This distinction stems from the up and rising "bring-your-own-device policies", which allow an employee to conduct business through their personal devices. Fifth, the law makes clear that it only protects "personal" accounts.[98] This will force Maryland courts to distinguish between what is considered a "personal" and nonpersonal account.

---

[92] Legislation Roundup: Maryland "Facebook Law" Raises New Obstacles for Employers and Other Significant Maryland Developments, jdsupra.com, http://www.jdsupra.com/legalnews/legislation-roundup-maryland-facebook-42390/ (last visited December 2, 2012)
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *Id.*

Furthermore, the act only restricts an employer from seeking an employee's login credentials. It does not bar an employer from asking an employee to login so they can view the online account. In addition, it does not bar employers from asking an applicant or employee to reproduce the online account, through printing or any other means. Lastly, the law does not prevent employers from viewing restricted information from an employee or applicant's online account through a coworker or other third party.[99]

2. ILLINOIS

Governor Pat Quinn of Illinois quickly followed in the footsteps of Governor Martin O'Malley in passing a bill making it illegal for employers to request private information from both employees as well as potential employees.[100] The law, which will take effect in January of 2013, is tough on employers and leaves no loopholes or exceptions that employers may utilize. According to Governor Quinn, the purpose of this law is to protect the privacy of individuals, as well as keep the law in pace with the rapid growth of technology.[101]

The new law prohibits employers from 1) Requesting or requiring that any employee or applicant provide their passwords, or "related account information," to any social networking site to an employer who wants to gain access to that account; or 2) Demanding access "in any manner" to an employee's or applicant's account or profile on a social networking website.[102] Unlike the Maryland law that has recently taken effect, this amendment to the Illinois Right to

---

[99] *Id.*

[100] Illinois' New "Facebook Password" Law May Create a Host of Unintended Consequences for Employers, jdsupra.com, http://www.jdsupra.com/legalnews/legislation-roundup-maryland-facebook-42390/ (last visited December 2, 2012).

[101] *Id.*

[102] *Id., See Illionois General Assembly Public Act 097-0875,* http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=097-0875 (last visited December 7, 2012).

Privacy in the Workplace Act incorporates little wiggle room for employers.[103] Effectively, unless the user makes their account information public, the employers are prohibited from seeking access to its content, regardless of the employers' intentions.

Because the only thing that the new law does not prohibit is the ability for employers to research information through the web that is already unrestricted by the privacy settings of the website, the act has stirred up some controversy, due to its additional, and perhaps unintentional, consequences.[104] For example, any employers who are involved in regulatory compliance measures and investigations will have difficulty doing their job with this law in effect. Secondly, employers who do a bulk of their business through these social media sites, which is increasing in number, will have difficulty in investigating employee misconduct that occurs through these channels.[105]

This act may also clash with the Illinois Freedom of Information Act (FIOA).[106] Due to the sweeping language of the new act, public employees may be prevented from fulfilling their duties under FOIA. For example, under the new law, public employers are prohibited from accessing records on personal devices, such as text messages. Yet under FOIA, it has been held that text messages sent by a public official are accessible, because they are used by the "public body".[107] So while the new act fulfills its purpose in restricting employers from accessing personal account information of all employees and applicants, there is some worry that it is too broad and may be over inclusive.

---

[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] *Id.*

CONCLUSION

Employers ought to be careful when soliciting social media network login information as a background check for prospective employees. Though the risks are currently ambiguous, they are increasing rapidly as potential federal and state laws restricting or regulating such behavior are emerging. Even without these potential federal and state laws, discrimination claims may make employers liable based on their hiring decisions. Social networking sites store various types of demographic information, which can cause employer liability for failure to hire or wrongful termination.

The digital age has given way to ever changing technologies, rapidly altering the way we function as a business society. Social media plays a large role in how we as a society interact, both in and out of the workplace. As current laws continue to play "catch-up" with technology and social media, no federal laws pointedly address this issue as of yet, making it possible for employers to engage in these invasive employment practices without penalty, and without remedy to applicants or employees. Although applicants and employees may find recourse in the SCA and CFAA, their case will be a difficult one to try. All the while, employees too frightened to lose their jobs have likely succumbed, giving up their privacy rights in exchange for their paycheck.

However, with new federal and state laws specifically addressing this issue, these practices will most likely be prohibited as a blatant violation of an employee's right to privacy. Although various states have passed new laws providing protection, these laws are not uniform, and some may be overly sweeping. Emerging federal laws such as SNOPA will give employees a voice in seeking protection for their social media account information. Unfortunately whether, and to what extent, employers can request employee and applicant login information remains

unresolved. Until federal legislation is passed, employees and potential employees will have a crucial decision to make: their privacy, or their paycheck.