SOCIAL MEDIA PRIVACY: WHAT'S IN A PASSWORD? – RIGHTS AND PROTECTION

By

Elizabeth A. Cameron, Dawn Swink, Kelsey Blades, and Mason Molesky*

In a world increasingly obsessed with updates such as "Mike Martin wants to be friends on Facebook" and "Jessica Jones likes your status," it is difficult to differentiate between public life and private life and to determine what information safely belongs to which realm. Usually we like to think that our private lives and our work lives have their own domains on the Internet, that our Facebook accounts do not affect our business lives. But the recent question for employees is not necessarily, "Do I want my friends to see that photo and tease me at work tomorrow?"—it is, "Does my employer have the right or the authority to see this information?" Even job applicants might ask, "Can the interviewer look at my Facebook account during the hiring process?"

Yes, this ambiguity has been the grim and present reality for the employment-possessing or employment-seeking social networking world. Beginning in 2011, employers—current as well as prospective—have gained media attention for requesting passwords to employees' accounts to social media sites such as Facebook and Twitter.[1] But the controversy extends past asking for log-in information. According to statistics, some users have been refused positions due to information posted on their social networks, and other individuals have been terminated based on status updates on Facebook.

However, this scenario is rapidly changing. New legislation, both state and federal, is underway as awareness of the privacy issue concerning social media and employment spreads and gains support. Several states have already forbidden employers from asking for passwords;[2] other states have legislation in the works,[3] and federal acts have been proposed to Congress.[4] The greatest block to social media privacy for employees appears to be the wait, however long, for congressional and presidential approval of federal legislation. Once that goal is reached employees and applicants will be able to rest assured, knowing that their social media passwords and login information are safe.

It is necessary to make an important distinction between two similar issues in this area. One involves viewing the public information posted on a candidate's or employee's social media account; the other involves requesting login information to view content that the user has chosen not to share with the public. While this article specifically addresses the latter issue, the former is also significant to the debate. Although the increase of social media legislation centers upon the protection of employees' login information, it must be kept in mind that employers and interviewers are breaking no laws by reading the content on a social media profile that is unprotected, that is, publicly available.

Additionally, the National Labor Relations Board has taken more proactive measures in guaranteeing an employee's right to speech concerning workplace conditions. In the past, employers have made a habit of formatting their social media policies to prohibit employees from discussing company matters publicly and from disparaging coworkers, managers, and the company itself.[5] However, recent rulings by the Board have restricted the degree to which employers can control what employees say online about their companies. These rulings,

> which apply to virtually all private sector employers, generally tell companies that it is illegal to adopt broad social media policies—like bans on "disrespectful" comments or posts that criticize the employer—if those policies discourage workers from exercising their right to communicate with one another with the aim of improving wages, benefits or working conditions.[6]

Denise M. Keyser, a labor lawyer, has recommended that companies use specific rather than blanket terminology to describe to employees exactly what type of information must not be posted—for example, private health information and trade secrets are to remain undisclosed, whether outside the office or online.[7] By doing so, employers are restricted from arguing that almost any negative post by an employee violates the social media policy, which serves to better protect the employee's online privacy. Such rulings demonstrate that employees' comments about their workplace will remain connected to social media sites and that steps will be taken to protect their rights online.

This paper provides an overview of the problems related to social networking sites, focusing on Facebook, and employee privacy. It discusses case examples of the consequences of posting information on a Facebook profile as well as how that information can affect the user's occupation status. This article explores the positions of Facebook and the diversity of opinion by employers and legal experts, as well as the legislative attempts at both the state and federal levels to prevent employees' privacy violation and the impact of this "American" problem on other nations.

Pre-legislation Cases

Although it may seem that most employers would not discriminate against applicants or terminate employees based on social media content, examples have surfaced demonstrating otherwise. The media have given attention to at least four cases that connect an employee's termination with content posted on a social media site.

Bland v. Roberts[8] began in 2009, when the defendant, Hampton, Virginia Sheriff Roberts, was running for reelection. Six deputy sheriffs, Bobby Bland, Daniel Ray Carter, Jr., David W. Dixon, Robert W. McCoy, John C. Sandhofer, and Debra H. Woodward, clicked "like" on the Facebook page of Roberts's political opponent during the election, titled simply "Jim Adams for Hampton Sheriff."[9] After Roberts won the election, he fired the six deputies. According to the deputies' appeal brief, Roberts warned them before the election "that they stay off the Facebook page of his opponent, which they said indicated their firings were linked to their social-media actions. Roberts told the Associated Press that the terminations resulted from poor job performance and that their actions online 'hindered the harmony and efficiency of the office.'"[10]

Interestingly, U.S. District Court judge Raymond Jackson granted the defendant's motion for summary judgment. According to the case brief, "[i]t is the Court's conclusion that merely 'liking' a Facebook page is insufficient speech to merit constitutional protection."[11] In arriving at this conclusion, the Court examined other cases, *Mattingly v. Milligan*[12] and *Gresham v. City of Atlanta*[13] that involved social media posts and the First Amendment right to free speech. The difference between *Mattingly* and *Gresham* and *Bland* is that the former two cases involved posted statements on Facebook profiles that the Courts were able to access; in Bland, however, the Court was unable to find evidence of posted content on Jim Adams's page—the only sign of affirmative content on Adams's page was the "like." Given these circumstances, Jackson decided that "[s]imply liking a Facebook page is insufficient [to qualify for First Amendment protection]. It is not the kind of substantive statement that has previously warranted constitutional protection."[14]

In February 2012, Nai Mai Chao worked as a nursing assistant at the Regency Gresham Skilled Nursing and Rehabilitation Center in Portland, Oregon. She allegedly received via text message photos of dying nursing home patients and the contents of the bedpans which they had used. Chao posted the photos to a board on her Facebook profile and gave them demeaning captions. A coworker took offense and notified Chao's supervisors, and she was consequently arrested and convicted of invasion of privacy. After her release on March 2, 2011, from an eight-day stay in jail, she lost not only her job but her nursing license as well.[15] Thus, although Chao only posted and captioned some photos on her Facebook profile, she was arrested, taken to court, convicted, terminated, and prohibited from working in that employment sphere. This case demonstrates the level of damage that can be done to an individual's career simply because of online content.

USA Today ran an article in April 2012 about former Marine Sergeant Gary Stein, who violated military rules by posting his extreme distaste for President Barack Obama on Facebook. In one online debate with approximately 29,000 followers, Stein wrote, "As an active duty Marine, I say screw Obama and I will not follow any orders from him [;] I will not salute him [;] Obama is the enemy."[16] Although it may seem that this post should have been constitutionally protected under Stein's First Amendment right to free speech, as argued by Bland, et al., against Roberts, such a defense would not have worked in Stein's situation because that rant violated Article 134 of the Uniform of Military Justice, which "bars behavior that harms the 'good order and discipline in the armed forces' or brings 'discredit on the armed forces.'"[17] In addition, the Defense Department "explicitly bars active-duty personnel from publishing 'partisan political articles, letters or endorsements signed or written by the member that (solicit) votes for or against a partisan political party, candidate or cause,'" and "any reasonable definition of 'publish' includes publicly posting an opinion where some 29,000 followers can read it."[18] The case would have been different if Stein had posted the comment on his private profile; however, since he had not, the Marine administrative panel advised giving Stein an "other than honorable" discharge for his behavior, which he received from Brigadier General Daniel Yoo on April 25, 2012.[19]

An even more recent instance is Denise Helms, a twenty-two-year-old former Cold Stone Creamery employee who was terminated after her Facebook status concerning the presidential election last November garnered media attention. Helms's status read: "And another 4 years of the (n-----). Maybe he will get assassinated this term..!!"[20] Chris Kegle, the store director of the Cold Stone where Helms worked, said he received more than twenty angry voicemails concerning Helms the morning after the story broke on Fox 40 news. He since relieved Helms from her position, stating that her views did not correlate to those of the creamery and that she was terminated due to her comments as well as the community's disapproval.[21] In addition, Helms's case will also be investigated by the Sacramento branch of the Secret Service. Section 871 of the U.S. Code lists threats against the President as a felony.[22]

Doubtlessly, these individuals had not expected that their posts or likes on their personal Facebook pages would cost them their jobs, professional licenses, or military ranks. And yet their actions had those results. These cases demonstrate all too clearly the blurring of lines between public and private life and even how purportedly "personal" content can interfere with a user's employment. The importance of ensuring that social media profiles are protected has already been discussed. An expectation to privacy exists only if profiles and posts have been set to "private," meaning that only "friends" of the user can view them. However, even that may not be enough. Helms had reportedly set her post about Obama to "private," but an individual who saw it took a screenshot and posted it to Twitter, which in turn captured the media's attention.[23] In addition, Chao's photos and comments were reported because a coworker saw them online, became offended, and notified their

supervisors. Thus, although a user can significantly protect herself by increasing the privacy settings on her social media profiles and accounts, she still needs to be aware that her posts are not 100 percent private; any individual with access to the profile can view the content posted and, as in the cases of Helms and Chao, may use them and take action.

The Beginning of the Legislation Push

While employees have faced employment-related consequences for their social media posts since allegedly, 2009, the call for legislation to protect employees' right to online privacy does not really occur until early 2011. In February of that year, Robert Collins experienced some difficulties in reapplying for a position, which initiated the subsequent national dispute regarding employees' account access information.

Collins was a Maryland corrections officer reapplying for his position in February 2011 after a four-month leave of absence. According to his testimony, he had to undergo a recertification process:

> The process progressed smoothly and without incident until my sit-down interview with the investigator at DOC's Centralized Hiring Unit.
> . . . During his course of questioning I was stunned to be asked a question which was new, and in my opinion, invasive and illegal. The investigator asked me if I had any social media accounts. I responded honestly and told him yes, as I intended to be forthright, transparent and cooperative in the process, as I needed my job in order to be able to provide for my family. He then proceeded to ask me which social media sites I was a member of. I told him that I only had a Facebook page. He then said, "what is the password." [sic] I said, "you can't be serious." He said, "I am serious as a heart attack." I did [sic] not want to do it, but because I really needed my job and he implied that this was a condition of recertification, I reluctantly gave him the password. He then proceeded to login to my account using my private credentials. I asked him, why are you logging onto my account and what are you looking for, what are you doing? With the back of the computer facing me, he said I am looking through your messages, on your wall and in your photos to make sure you are not a gang member or have any gang affiliation. I was mortified.[24]

In a news article, Collins reports, "I was sitting there in a state of awe. [The interviewer] basically implied my collaboration was compulsory."[25] Afraid he would not be given the position, Collins handed over the information. Later, he contacted the local chapter of the American Civil Liberties Union, which in turn protested to the Maryland Department of Public Safety and Correctional Services.

In April 2011, the Department of Corrections changed its policy. Instead of asking for prospective employees' passwords, interviewers may ask applicants to log on to their accounts during interviews.[26] Soon after, Maryland Senator Ronald Young introduced legislature to push for social media privacy legislation.

Employer and Employee Arguments

When reports of the difficulties faced by Robert Collins and other employees broke, Facebook took a defensive position and protected the privacy rights of the employees while disagreeing with employers who asked for account access information. Facebook Chief Privacy Officer Erin Egan issued a statement on March 23, 2012, responding to the complaints, part of which reads:

> In recent months, we've seen a distressing increase in reports of employers or others seeking to gain inappropriate access to people's Facebook profiles or private information. This practice undermines the privacy expectations and the security of both the user and the user's friends. It also potentially exposes the employer who seeks this access to unanticipated legal liability.
>
> The most alarming of these practices is the reported incidents of employers asking prospective or actual employees to reveal their passwords. If you are a Facebook user, you should never have to share your password, let anyone access your account, or do anything that might jeopardize the security of your account or violate the privacy of your friends. We have worked really hard at Facebook to give you the tools to control who sees your information. . . . That's why we've made it a violation of Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password.
>
> [. . .]

> Facebook takes your privacy seriously. We'll take action to protect the privacy and security of our users, whether by engaging policymakers or, where appropriate, by initiating legal action, including by shutting down applications that abuse their privileges.[27]

Later that day, Egan issued a new statement clarifying one of the terms in this last-mentioned paragraph of the original statement. The new statement reads:

> We don't think employers should be asking prospective employees to provide their passwords because we don't think it's the right thing to do. While we do not have any immediate plans to take legal action against any specific employers, we look forward to engaging with policy makers and other stakeholders, to help better safeguard the privacy of our users.[28]

Although Facebook has, it seems, toned down its aggressiveness on prosecuting those who violate its privacy policy, it remains concerned with each user's privacy rights and seeks to discourage employers from requesting login information. The site's director for state public policy, Will Castleberry, said in a statement, "Asking employees or job applicants for their passwords is wrong."[29] It does not appear that Facebook is likely to accede to employers' interests anytime soon.

Employers themselves, however, seem to entertain differing opinions on checking policies. Job website CareerBuilder.com conducted a survey of more than 26,000 hiring managers in 2009. The results "indicated that 45 percent of employers used a social networking site to vet potential employees—more than double the percentage in 2008, and a step in a direction officials say likely won't change anytime soon."[30] Indeed, according to Lester Rosen, who serves as founder and CEO of Employment Screening Resources, "Employers are wrestling with [the debate over virtual background checks] . . . Some employers won't do it, other employers won't hire without it."[31] CareerBuilder's senior career advisor, Ryan Hunt, said, "Social media has become integral to how we communicate, and as a result, there are an increasing number of employers using these sites to screen candidates."[32]

Reverting to a point made earlier in the paper, a distinction must be made between an employer's examination of publicly accessible social media content and an employer's request for login information in order to view protected information and content. Privacy settings had been no barrier for the Virginia State Police, who adopted the policy of utilizing social media accounts for the purpose of background checks. The American Civil Liberties Union of Virginia filed a complaint against the state police in late March 2012.[33] The point remains that employers appear to be divided on requesting login information. Some employers believe it to be unethical; others, such as Virginia state police spokeswoman Corinne Geller, believe that such a request is now "a necessary part of the overall background investigation process."[34]

Those with legal experience seem divided on the issue as well. Elizabeth Torphy-Donzella, a labor and employment attorney, worked for the Maryland Chamber of Commerce to oppose a Maryland bill which prohibited employers from requesting employees' and applicants' credentials. She said the bill "[took] away important access for employers who need to investigate harassment claims and other misconduct" and "was drafted in a manner that didn't take account of legitimate employer needs to request access to employee Facebook pages."[35] On the other hand, Maryland social media attorney Bradley Shear "argues that the legislation is good for businesses because it prevents them from being liable for information, such as criminal or harassing behavior, that they could discover when reviewing employee profiles."[36] He said that such action creates "tremendous legal liability"[37] for companies and schools who request login information: "litigants [may find it difficult] to claim that these entities have a legal duty to monitor the personal digital accounts of their employees and/or students."[38]

Although Torphy-Donzella raises a valid point concerning the usefulness of employers' having access to employees' social media accounts, that issue does cross a boundary that is different from the current debate and direction of the legislation. While an employer may indeed benefit from accessing employees' social media accounts in order to look into misconduct claims, that issue is distinctly different from the employer's use of social media account login information to perform virtual background checks and to monitor general account information. If an employee were to complain to her employer about harassment via social media, one would think that she would be willing to log in to her social media account and show the contents to her employer. This is different from employers requiring employees to log in to their profiles, which would be prohibited under the Maryland bill. Furthermore, in that case, the employer need not require or simply ask the accused employee to log in, because the alleged victim should have access to the offensive content and can show that to the employer. In addition, if an employee is harassing another online, the employer may be able to detect traces of that harassment in the workplace, to which the online content may only be supplemental. So, while Torphy-Donzella's concern about the ability of employers to look into harassment complaints is legitimate, it does not follow that forbidding employers to request social media account information will interfere with that goal.

Current and Pending Protective Legislation

Given the current problems concerning the use of social networking sites and its applicability to the employment sphere, it seems wise to begin with general privacy laws regarding the workplace since privacy is at the heart of the issues between employers and their employees who use social networks.

The general rule is that if an employer has provided an employee with some article of property, such as a car, a desk, an office, a locker, or a computer, the employer has the right to search the property because she provided it to the employee.[39] Likewise, since the e-mail system used by employees belongs to the employer, the employer has the right to read the employees' e-mails.[40] Thus, employees should generally assume that their rights to privacy at work are limited.

> Courts tend to follow a general pattern when it comes to deciding cases involving employee privacy by weigh[ing] the employer's interests against the employee's reasonable expectation of privacy. Normally, if employees have been informed that their communications are being monitored, they cannot reasonably expect those communications to be private. If employees are not informed that certain communications are being monitored, however, the employer may be held liable for invading [employees'] privacy.[41]

Given the prevalence of online interactions, employers must abide by the Electronic Communications Privacy Act (ECPA) of 1986, the title of which commonly refers to both the ECPA of 1986 and the Stored Wire Electronic Communications Act.[42] The main purpose of the EPCA is to protect "wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to e-mail, telephone conversations, and data stored electronically."[43] Title 1 of the Act "prohibits the intentional actual or attempted interception, use, disclosure, or 'procure [ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.'"[44] Regarding the general privacy laws at work, however, the ECPA does not cover "any electronic communications through devices that are 'furnished to the subscriber or user by a provider of wire or electronic communication service' and that are being used by the subscriber or user, or by the provider of the service, 'in the ordinary course of its business.'"[45]

Following Robert Collins's and the ACLU's complaint to the Maryland Department of Public Safety and Correctional Services, that state has emerged as one of the first to take legislative action to protect the privacy of employees' personal social networking accounts. Legislation banning employers from requesting or requiring *either* current or prospective employees to give out log-in information to sites like Facebook passed in April 2012.[46] This legislation, then, has set an important precedent regarding the rights of employees to online privacy.

Other states have followed suit to protect employees—prospective as well as current—from forcibly giving over their required login information for their social media accounts. Illinois and California passed legislation in August and September 2012, respectively, which prohibits employers from demanding usernames and passwords from employees and applicants, and California and Delaware have banned institutions of higher education from asking the same information from students and applicants.[47] According to the National Conference of State Legislatures, by May 2013 thirty-five states have either pending legislation or introduced legislature regulating the ability of employees and/or schools and universities to request or demand access information to social network accounts.[48] This number has increased from eleven states in December 2012, which demonstrates that more lawmakers support employees' and applicants' rights to privacy concerning the private content on their social media profiles.

The federal government has also addressed this issue. In March 2012, Democratic Congressman Ed Perlmutter sought to add an amendment to the Federal Communications Commission Process Reform Act of 2012; however, the Republicans largely opposed the proposal. The final vote came in at 236 to 184, with one House Republican voting in favor and only two House Democrats voting against the proposal.[49] The amendment would have read as follows:

> Nothing in this Act or any amendment made by this Act shall be construed to limit or restrict the ability of the Federal Communications Commission to adopt a rule or to amend an existing rule to protect online privacy, including requirements in such rule that prohibit licensees or regulated entities from mandating that job applicants or employees disclose confidential passwords to social networking websites.[50]

The Republicans said that although they felt that the amendment was unnecessary, they would be willing to work on legislation with a similar aim in the future.[51]

In addition, Democratic Senators Charles E. Schumer and Richard Blumenthal have asked Attorney General Eric Holder to look into the issue and to determine whether the requests of employers for employees' login information violate federal law. They are specifically interested in whether "this practice violates the Stored Communications Act or the Computer Fraud and Abuse Act."[52] The first "prohibit[s] intentional access to electronic information without the authorization" and the second forbids "intentional access to a computer without authorization to obtain information."[53]

Further proposals for federal legislation came from Democrat Representatives Eliot Engel and Jan Schakowsky, who introduced the Social Networking Online Protection Act (SNOPA) bill to Congress in April 2012. If passed, a press release on Engel's website said SNOPA will "prohibit current and potential employers for requiring a username, password or other

access to online content."[54] SNOPA would impose the same limitation on educational institutions from the kindergarten to the university level. The bill has seven sponsors (six Democrats and one Republican) and was referred to the House Education and the Workforce committee on February 6, 2013, "which will consider [the bill] before possibly sending it on to the House or Senate as a whole."[55]

However, SNOPA's prognosis gives the bill a one percent chance of getting past the committee and a zero percent chance of being enacted.[56] This establishes that hesitancy still exists within Congress with regard to passing federal legislation prohibiting employers from requiring employees' social media login information. The vast majority of Republican representatives voted against Perlmutter's amendment to the Federal Communications Commission Process Reform Act of 2012, and the House Education and the Workforce committee consists of twenty-three Republicans and eighteen Democrats.[57] Although the likelihood of SNOPA's getting past the House committee is very low, perhaps the committee members will be able to sort through the bill's issues and benefits discussed by both parties and will, in time, report the updates to the rest of Congress. While prospects are dim that the report will be made relatively soon, at least state legislatures are taking the initiative to protect employees and applicants.

International Perspective

Word of the complicated employment-Facebook-privacy triangle has spread to other nations as well, who have begun to experience similar issues. As Sarah Veale, head of equality and employment rights at the Trades Union Congress in Britain, said, "Once something like this starts happening in the US, it is likely to come over here—especially in American businesses which have outposts in [the] UK. If interviewers in the US are adopting this practice of asking prospective staff for access to their Facebook accounts, they will start doing it over here."[58] Canada has also been affected by the social media privacy situation.

Veale is correct about the new American-based issues facing Britain. In *Flexman v BG Group*, former human resources executive John Flexman brought suit against his former employer, BG Group, in January 2012, alleging that he had been fired after posting his curriculum vitae on his LinkedIn profile.[59] In addition, online retail worker Lee Williams told British newspaper, *The Telegraph*, that his managing director asked for Williams's Facebook login information after looking him up on the site and finding that he was unable to view Williams' profile. When Williams refused, the director "persisted with his request, but then let it go without taking any further action."[60]

It is not clear at present how much latitude Britain's laws will afford employers. However, given the recent situation, it seems likely that the issue will create controversy. Experts in Britain say that "there is nothing to stop UK employers 'at least asking the question'" for social media passwords, and employment attorney Paula Whelan said "it would be very difficult to prove discrimination if a candidate thought they didn't get a job because they refused to hand over their login details."[61] She is correct, and statistics may be of little avail in proving such discrimination.

In 2011, after Robert Collins's complaint, the Maryland Department of Corrections reviewed its application process for correctional officers and other security-sensitive positions. The review found that refusing to relinquish log-in information bore no ill consequences: there was "no indication that an applicant's refusal to share social media information had a negative impact on the applicant's chances of employment."[62] Although they are transnational, these statistics support Whelan's notion of the difficulty of proving discrimination based on willingness to share social media access information. Thus, it seems that Britons may be in an uncomfortable situation, as there currently is little protection for employees pertaining to social media privacy.

Canada has also established legal protection for prospective employees from prying employers. Lawyers interviewed by *The Globe and Mail* said that "[l]abour laws in Canada offer strong protection from employers who ask job seekers for personal information such as social media passwords."[63] Toronto-based labor attorney Paul Cavaluzzo said "there is little need for Canada to follow suit" of the United States and initiate legislation banning the practice. "In Canada we've always respected privacy rights, which means that the employer does not have, and should not have, access to personal information."[64]

Conclusion

As of September 30, 2012, Facebook registered a total of 166,029,240 users in the United States alone.[65] Social media networking is a major component of life in the United States and around the world, and it is unlikely this will change anytime soon. At the same time, these users are graduating and entering the workforce. Employers will always want to interview and hire the best candidates for the positions they offer, and profiles on social media sites such as Facebook are available to provide insight into the backgrounds of those candidates.

In terms of an employer's asking for an employee's account access information, the conflict between an employer's right and the employee's right to privacy remains to be settled, but advocates of online privacy have gained several advancements over the past few months. Facebook's personal disapproval of employers' requests for passwords to accounts on its site and new state laws are a step in the right direction to shield employees' private information. In addition, if pending federal

legislation makes it past the House of Representatives, the Senate, and the President of the United States, it looks as though employers may be barred from asking for employees' and applicants' passwords altogether.

However, it is important that social media users recognize their own responsibility in assuring that their employment or application status is not threatened. Although state and federal laws can prevent employers and interviewers from asking for login information, a user's posted content may still be visible if he neglects to raise his privacy settings. An employer need not ask for a password if she can find telling status updates, comments, and other posts after a quick search. Therefore, the wisest move employees can make while awaiting legislative enactment is to stand up for their own privacy by heightening their profiles' security. By enhancing privacy protection, employees are doing their part to ensure the privacy of their online and personal lives.

---

*Professor of Business Administration, Alma College, Associate Professor of Business Law, University of St. Thomas, Kelsey Blades, Alma College Student, and Mason Molesky, Alma College Student.

Footnotes

[1] *See e.g.*, Manuel Valdes and Shannon McFarland, *Employers Asking Job Seekers for Facebook Passwords*, BOSTON GLOBE, Mar. 21, 2012, http://www.bostonglobe.com/business/2012/03/20/employers-asking-job-seekers-for-facebook-passwords/QxviQzYrVRxW8UVFw1MGRI/story.html (last accessed May 13, 2013).
[2] The states with enacted statutes are: Arkansas, California, Colorado, Illinois, Maryland, Michigan, New Mexico, Oregon, Utah, Vermont and Washington (statutes' cites omitted).
[3] Those states are: Arizona, Connecticut, Delaware, Georgia, Hawaii, Iowa, Kansas, Louisiana, Maine, Massachusetts, Minnesota, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Rhode Island, South Carolina, Texas, and West Virginia (legislative citations omitted). It should be noted that bills brought forth in both North Dakota and Mississippi either failed or died in committee.
[4] *See infra*, footnotes 47-55 for a discussion on this movement.
[5]Steven Greenhouse, *Even if It Enrages Your Boss, Social Net Speech Is Protected*, N.Y. TIMES, Jan. 21, 2013, http://www.nytimes.com/2013/01/22/technology/employers-social-media-policies-come-under-regulatory-scrutiny.html (last visited May 30, 2013)
[6] *Id*.
[7] *Id.*
[8] 857 F.Supp.2d. 599 (E.D. Va. 2012).
[9] Doug Gross, *Virginia Deputy Fights his Firing over a Facebook 'Like,'* CNN, Aug. 13, 2012, http://www.cnn.com/2012/08/10/tech/social-media/deputy-fired-facebook-like (last visited May 30, 2013).
[10] Mark Guarino, *Could 'Liking' Something on Facebook Get You Fired?*, CHRISTIAN SCI. MONITOR, Aug. 10, 2012, http://www.csmonitor.com/USA/Justice/2012/0810/Could-liking-something-on-Facebook-get-you-fired (last visited May 30, 2013).
[11] Brief at 6, *Bland v. Roberts*, No. 4:11cv45 (United States District Court Eastern District of Virginia, Newport News Division Apr. 24, 2012).
[12] 2011 U.S. Dist. LEXIS 12665 (E.D. Ark). Nov. 1, 2011).
[13] 2011 U.S. Dist. LEXIS 116812 (N.D. Ga.) Sept. 29, 2011).
[14] *See supra* note 11.
[15] Meredith Bennett-Smith, *Job Interviewer Asks for Facebook Password. Should You Give it?*, CHRISTIAN SCI. MONITOR, June 11, 2012, http://www.csmonitor.com/Business/2012/0611/Job-interviewer-asks-for-Facebook-password.-Should-you-give-it/(page)/2 (last visited May 30, 2013).
[16]*Marine's Facebook Rants Earn Ticket out of the Military*, USA TODAY, Apr. 13, 2012, at 8A.
[17] *Id*.
[18] *Id*.
[19] Michael S. James and Marisa Taylor, *Marine Sgt. Gary Stein Gets 'Other Than Honorable' Discharge Over Anti-Obama Facebook Comment*, ABC NEWS, Apr. 25, 2012, http://abcnews.go.com/US/marine-sgt-gary-stein-honorable-discharge-anti-obama/story?id=16216279#.UXl-fG3D-00 (last visited May 30, 2013).
[20] Marijke Rowland, *Obama threat gets Turlock Woman Fired, Reported to Secret Service*, MODESTO BEE, Nov. 8, 2012, http://www.modbee.com/2012/11/08/2448491/obama-threat-gets-woman-fired.html (last visited May 30, 2013).
[21] *Id*.
[22] *Id.*
[23] Jason Howerton, *This Woman Lost Her Job Over a Facebook Post—And You Won't Believe What She Said about Obama*, THE BLAZE, Nov. 9, 2012, http://www.theblaze.com/stories/2012/11/09/this-woman-lost-her-job-over-a-facebook-post-and-she-deserved-it/ (last visited Apr. 25, 2013).

[24] *See* Robert Collins's testimony, http://www.aclu-md.org/uploaded_files/0000/0176/collins_testimony.pdf (last visited May 30, 2013).
[25] *See supra* note 15.
[26] *Maryland Becomes First State to OK Facebook Password Protection Bill*, HUFFINGTON POST, Apr. 22, 2012, http://www.huffingtonpost.com/2012/04/20/maryland-becomes-first-st_n_1439866.html (last visited Dec. 9, 2012).
[27] Erin Egan, *Protecting Your Passwords and Your Privacy*, FACEBOOK, Mar. 23, 2012, http://www.facebook.com/note.php?note_id=326598317390057 (last visited May 30, 2013).
[28] Michelle Maltais, *Facebook Softens its Stand on Bosses Violating Applicant Privacy*, L.A. TIMES, Apr. 23, 2012, http://articles.latimes.com/print/2012/mar/23/business/la-fi-tn-facebook-softens-its-stand-20120323 (last visited May 30, 2013).
[29] *See supra* note 26.
[30] Somers, *Employers Differ on Checking Online*, WASHINGTON TIMES, Apr. 4. 2012, at 16, § A.
[31] *Id*.

[32] *Id*.
[33] *Id*.
[34] *See id*.
[35] *Maryland Becomes First*, *supra* note 26.
[36] *Id.*
[37] *See id.*
[38] Bradley Shear, *Right to Privacy Will Be Protected by the Social Networking Online Protection Act*, SHEAR ON SOCIAL MEDIA LAW BLOG (Feb. 18, 2013), http://www.shearsocialmedia.com/2013/02/right-to-privacy-will-be-protected-by.html (last visited May 12 2013).
[39] *Privacy at Work: What Are Your Rights?*, FINDLAW.COM, http://employment.findlaw.com/workplace-privacy/privacy-at-work-what-are-your-rights.html (last visited Dec. 9, 2012).
[40] *See Id.*
[41] R. MILLER & G. JENTZ, BUSINESS LAW TODAY, 619 (9th ed. 2011).
[42] *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §2510-22*, http://www.it.ojp.gov/default.aspx?area=privacy&page=1285 (last visited Dec. 9, 2012).
[43] *See id.*
[44] *See id.*
[45] *See supra* note 26.
[46] *See supra* note 26.
[47] *See* National Congress of State Legislatures, *Employer Access to Social Media Usernames and Passwords*, Nov. 16, 2012, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx (last visited May 30, 2013).
[48] *See id.*
[49] 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 (last visited May 30, 2013).
[50] *Id*.
[51] Emma Barnett, *Republicans Reject Legislation to Protect Facebook Users from Snooping Bosses*, THE TELEGRAPH, Mar. 29, 2012, http://www.telegraph.co.uk/technology/facebook/9172934/Republicans-reject-legislation-to-protect-Facebook-users-from-snooping-bosses.html (last visited May 30, 2013).
[52] Valdes, *Can Employers Ask for Applicants' Passwords?*, WASH. POST., Mar. 26, 2012, at A12.
[53] *Id*.
[54] Michelle Maltais, *SNOPA Bill Seeks to Keep Employers Out of Private Social Networks*, L.A. TIMES, Apr. 30, 2012, http://articles.latimes.com/print/2012/apr/30/business/la-fi-tn-federal-bill-bans-employers-seeking-facebook-password-20120430 (last visited May 20, 2013).
[55] H. R. 537: Social Networking Online Protection Act, http://www.govtrack.us/congress/bills/113/hr537 (last visited May 30, 2013).
[56] *See id*.
[57] *See* HOUSE COMMITTEE ON EDUCATION AND THE WORKFORCE, http://www.govtrack.us/congress/committees/HSED (last visited Apr. 25, 2013).
[58] Emma Barnett, *Facebook Passwords 'Fair Game in Job Interviews'*, THE TELEGRAPH, Mar. 23, 2012, http://www.telegraph.co.uk/technology/facebook/9162356/Facebook-passwords-fair-game-in-job-interviews.html (last visited May 30, 2013).
[59] *See id*.

[60] *Id.*
[61] *Laws to protect Facebook passwords from prying employers*, THE TELEGRAPH, Apr. 30, 2012, http://www.telegraph.co.uk/technology/facebook/9235869/Laws-to-protect-Facebook-passwords-from-prying-employers.html (last visited May 30, 2013).
[62] Press Release, Md. Department of Public Safety and Correctional Services (Apr. 6, 2011) (detailing changes in the social media inquiry policy for correctional officer applicants), http://dpscs.maryland.gov/publicinfo/news_stories/press_releases/20110406a.shtml.
[63] McQuigge, *Company Wants your Facebook Password? Just Say No*, GLOBE AND MAIL, Mar. 28, 2012, at B19.
[64] *Id.*
[65] *See Internet Usage, Facebook Subscribers and Population Statistics for all the Americas World Region Countries*, June 30, 2012, http://www.internetworldstats.com/stats2.htm (last visited May 31, 2013). There have been a few reports that Facebook usage within the United States has been dropping. *See, e.g.*, *Juliette Garside and Dominic Rushe, Facebook Profits Rise Despite Drop in US Visitors to its Website*, THE GUARDIAN, May 2, 2013, http://www.guardian.co.uk/technology/2013/may/01/facebook-loses-10m-visitors-us (last visited May 31, 2013). However, this fails to take into account the number of new unique mobile users, not traditionally counted in desktop statistics. *See* Justin Lafferty, *U.S. Facebook Users Becoming More Mobile-Centric*, ALLFACEBOOK.COM, May 10, 2013, http://allfacebook.com/u-s-facebook-users-becoming-more-mobile-centric-b117162 (stating Facebook's desktop site had 142.1 million unique visitors as of March 2013 but Facebook's mobile app had 99 million U.S. unique users, an increase over the 62 million unique mobile users as of March 2012). *Id.*