NOTE

EMPLOYMENT, COLLEGE STUDENTS, & SOCIAL MEDIA, A RECIPE FOR DISASTER: WHY THE PROPOSED SOCIAL NETWORKING ONLINE PROTECTION ACT IS NOT YOUR BEST FACEBOOK "FRIEND"

*Hillary Gunther**

TABLE OF CONTENTS

* Hillary Gunther earned her J.D. from Albany Law School in 2014. At Albany Law, she served as Editor for the Symposium for the Journal of Science and Technology, as well as research assistant for the New York State Bar Association's Business Law Journal.

I. INTRODUCTION

With the ubiquitous presence of online social media and its usage in the modern era, an array of legislative challenges has emerged, including the dichotomy between the right to privacy and the ready availability of personal information via the Internet. The seemingly limitless capability of the Internet to store information begs the question now and going forward, is *anything* contained in private social media accounts actually private? And more importantly, *should* such information be private?

The Social Networking Online Protection Act (SNOPA)[1], a federal bill introduced into the House of Representatives on February 6, 2013, states that:

> It shall be unlawful for any employer to require or request that an employee or applicant for employment provide the employer with a user name, password, or any other means for accessing a private email account of the employee or applicant or the personal account of the employee or applicant on any social networking website; or to discharge, discipline, discriminate against in any manner, or deny employment or promotion to . . . any employee or applicant for employment because the employee or applicant . . . refuses or declines to provide [such information] . . .
>
> [Higher Education Institutions] will not require or request that a student or potential student provide the institution with a user name, password, or any other means for accessing a private email account of the student or potential student or the personal account of the student or potential student on any social networking

[1] H.R. 537, 113th Cong. (2013).

> website; or discharge, discipline, discriminate against in any manner, or deny admission to, suspend, or expel, or threaten to take any such action against, any student or potential student because the student or potential student refuses or declines to provide [such information] . . .
>
> No local [public] educational agency . . . may require or request that a student or potential student provide the agency or a school served by the agency with a user name, password, or any other means for accessing a private email account of the student or potential student or the personal account of the student or potential student on any social networking website; or discharge, discipline, discriminate against in any manner, or deny admission to, suspend, or expel, or threaten to take any such action against, any student or potential student because the student or potential student refuses or declines to provide [such information].[2]

The Act allows for civil penalties up to $10,000 for any employer who violates its provisions.[3] It provides that a determination of the appropriate amount of the penalty shall be based on both the track record of the employer in complying with SNOPA, as well as the severity of the particular violation.[4]

While at first blush, SNOPA appears to be an appropriate legislative solution addressing modern social media issues, it is in effect vastly under-inclusive in terms of the actual problems caused by such social media.[5] Concurrently, it is over-inclusive, as it imposes an outright ban on the practice of obtaining social media passwords by employers, notwithstanding the nature of the position or interests at stake.[6] In order to properly contextualize the likely ineffectiveness of the SNOPA, this Note will focus on Facebook. It will highlight prevalent issues caused by Facebook, zeroing in on various "Facebook firing" cases, as well as higher education Facebook monitoring. This Note will also discuss SNOPA's reach relative to prevalent "Facebook problems," as well as current legislative attempts to prevent inappropriate usage of information obtained through Facebook. This Note will provide arguments both for and against the conduct that SNOPA prohibits, and ultimately concludes that

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *See infra* Part VII (discussing the inadequacy of SNOPA).
[6] *See infra* Part VIII (examining situations in which employers should be allowed access to employees' social media).

SNOPA is not an appropriate or sufficient remedy to the primary issues. Moreover, it will discuss certain circumstances in which the conduct prohibited by SNOPA should not be prohibited. For the purpose of highlighting various arguments, the fact that an individual violates the Facebook Terms of Service by sharing her password or allowing another to access her account[7], will be ignored.

II. FOUNDATIONS OF PROTECTED EMPLOYEE SPEECH

The National Labor Relations Act permits employees to engage in protected concerted activity, such as on their own time, discussing working conditions or even criticizing managers or supervisors.[8] Since protected concerted speech is not rooted in the Constitution, all employees, public or private, are entitled to it.[9] However, protection of such speech is not limitless, and has been subject to interpretation as the nature of workplace activity and communications has changed.

In a landmark dispute, *Atlantic Steel Co.*,[10] an employee was terminated following a workplace outburst against his supervisor.[11] The National Labor Relations Board (hereinafter, "the Board") provided four factors to determine whether an employee was entitled to protection under the Act: "(1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee's outburst; and (4) whether the outburst was, in any way, provoked by an employer's unfair labor practice."[12] The Board determined that because the outburst occurred on the production floor during working hours and the employee reacted in an unreasonable and obscene manner, the reaction was not a result of provocation, and because such conduct was not normally tolerated in the particular work setting, the outburst was not protected under the Act.[13] Today,

[7] *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (November 15, 2013).

[8] David Alim-Young, *NLRB Weighs in on Social Networking – "The Facebook Complaint"*, NLRB INSIGHT (Feb. 8, 2011), http://www.nlrbinsight.com/2011/02/nlrb-weighs-in-on-social-networking-the-facebook-complaint; *see also* 29 U.S.C. § 157 (2012) (asserting employees' right of collective bargaining).

[9] Alim-Young, *supra* note 8.

[10] 245 N.L.R.B. 814 (Sept. 28, 1979).

[11] *Id.* at 814.

[12] *Id.* at 816.

[13] *Id.* at 816–17.

the *Atlantic Steel* analysis is generally applied where employees make public outbursts against a supervisor.[14]

In another decision that added to the framework for protected concerted speech, *N.L.R.B. v. Local Union No. 1229, Intern. Broth. Of Elec. Workers*[15] (hereinafter "Jefferson Standard"), the Supreme Court determined that "[t]he legal principle that insubordination, disobedience or disloyalty is adequate cause for discharge is plain enough."[16] In *Jefferson Standard*, several technicians employed at a broadcasting company attacked the quality of the company's television broadcasts.[17] Such attacks were manifested through handbills, and distributed on a public square a few blocks from the company's premises, as well as in local businesses and other public locations.[18] The handbills made no reference to collective bargaining, a labor controversy, or union activity.[19]

The Court held that the technicians lost protection under the Act, because the attack related to no labor practice of the company; made no reference to working conditions, hours, or wages; was aimed at the interests which the attackers were paid to develop and conserve; and was targeted toward matters of finance and public relations, areas for which management, and not the technicians, was responsible.[20] *Jefferson Standard* typically applies where an employee has made disparaging remarks about an employer that, in context, appeals to an outside or third party.[21]

Since *Jefferson Standard*,

> [T]he Board has held that employee communications to third parties in an effort to obtain his or her support are protected where the communication indicated it is related to an ongoing dispute between the employees and the employers and the communication is not so disloyal, reckless or maliciously untrue as to lose the Act's protection.[22]

That standard also applies to content posted on social media

[14] Memorandum OM-74 from Office of the Gen. Counsel Div. of Operations Mgmt. (Aug. 18, 2011).
[15] 346 U.S. 464 (1953).
[16] *Id.* at 475.
[17] *Id.* at 467–68.
[18] *Id.* at 468.
[19] *Id.*
[20] *Id.* at 476.
[21] Atlantic Steel Co., 245 N.L.R.B. 814, 816 (1979).
[22] Am. Golf Corp., 330 N.L.R.B. 1238, 1240 (2000).

sites.[23] A series of decisions by the Board clarified the scope of concerted activity, stating that an activity is concerted when the employee acts "with or on the authority of other employees, and not solely by and on behalf of the employee himself."[24] The type of communications protected under the Act have been described as "the same as [those discussed] at the water cooler."[25] Although the outlets for protected concerted speech have changed, the principals remain the same.

III. ISSUES RELATING TO SOCIAL MEDIA

A. Facebook Firing

Employment issues today that fall within the realm of the National Labor Relations Act often arise in the context of employee social media posts and photos. The social media activity of employees is subject to the same protected concerted speech criteria that are applied to other outlets of speech, such as the workplace floor or handbills in public locations.[26] The prevalence of lawsuits filed by discharged employees, resulting from content posted on Facebook, cannot be overstated. With over one billion Facebook users worldwide,[27] coupled with the arguably inadequate legislation governing content online, the prevalence of employment disputes resulting from information obtained from Facebook and other social media is unsurprising.[28]

According to a survey of 261 large U.S. companies, conducted by the Internet security firm, Proofpoint, 17% of companies with

[23] *See* Three D, LLC, No. 34-CA-12915, 2012 WL 76862 (N.L.R.B. Div. of Judges Jan. 3, 2012) (analyzing employee Facebook comments under the *Jefferson* standard).

[24] Meyers Indus., Inc. (*Meyers II*), 281 N.L.R.B. 882, 885 (1986) (quoting Meyers Indus., Inc. (*Meyers I*), 268 N.L.R.B. 493, 497 (1984)).

[25] Alim-Young, *supra* note 8; *see also* Ben DiPietro, *Will Employers Like NLRB Ruling on 'Virtual Water Cooler' Chatter?*, WALL ST. J. (Feb. 4, 2014, 7:04 AM), http://blogs.wsj.com/riskandcompliance/2014/02/04/the-morning-risk-report-will-employers-like-nlrb-ruling-on-virtual-watercooler-chatter-2.

[26] *See supra* Part II (discussing the limitations of protected concerted speech in the workplace).

[27] *Social Networking Statistics*, STATISTIC BRAIN, http://www.statisticbrain.com/social-networking-statistics (last visited Apr. 23, 2014).

[28] *See, e.g.*, Dylan Love, *17 People Who Were Fired for Using Facebook*, BUS. INSIDER (May 11, 2011, 6:13 PM), http://www.businessinsider.com/facebook-fired-2011-5?op=1 (highlighting various instances in which employees were terminated from employment for content they posted on Facebook).

1,000 or more employers reported issues with employees using social media, and 8% reported actually dismissing an employee for his or her behavior on social networking sites.[29] It found that of these same companies, 15% had disciplined an employee for violating multimedia policies and 17% had disciplined employees for violating message or blog board policies.[30] The rising number of disputes involving social media suggests that "these aren't just outliers, but the result of a serious crackdown by corporate America on tracking their employees' online activities."[31]

Generally, an employee's social media post is "protected concerted activity within the meaning of Section 7 of the National Labor Relations Act [if] it involve[s] a conversation among coworkers about their terms and conditions of employment, including their job performance and staffing levels."[32] In a recent decision, the NLRB held that employees of a restaurant, who posted comments on Facebook regarding both the employer's failure to properly prepare their tax returns, and the subsequent tax liability that followed, were engaged in protected concerted activity and were wrongfully discharged.[33] By clicking the "like" button, one employee expressed agreement with a comment by a former employee, "[m]aybe someone should do the owners of Triple Play a favor and buy it from them. They can't even do the tax paperwork correctly!!! Now I OWE money . . . Wtf!!!!"[34] Another comment by an employee stated "I owe too. Such an asshole."[35] The NLRB, in reaching its decision, noted that the subject matter of the Facebook posts was protected, as it involved the employer's calculation of employees'

[29] *Five Hospital Staffers Fired for Social Media Discussions*, PROOFPOINT (June 9, 2010, 12:38 PM), http://blog.proofpoint.com/2010/06/five-hospital-staffers-fired-for-social-media-discussions-about-patients.html; Adam Ostrow, *FACEBOOK FIRED: 8% of U.S. Companies Have Sacked Social Media Miscreants*, MASHABLE (Aug. 10, 2009), http://mashable.com/2009/08/10/social-media-misuse.

[30] Ostrow, *supra* note 29.

[31] *Id.*

[32] *Administrative Law Judge Finds New York Nonprofit Unlawfully Discharged Employees Following Facebook Posts*, NAT'L LABOR RELATIONS BD. (Sept. 6, 2011), http://www.nlrb.gov/news-outreach/news-releases/administrative-law-judge-finds-new-york-nonprofit-unlawfully-discharged.

[33] Three D, LLC, No. 34-CA-12915, 2012 WL 76862 (N.L.R.B. Div. of Judges Jan. 3, 2012).

[34] *Id.*

[35] *Id.* (referring to the employer).

taxes.[36] Moreover, the nature of the outburst was not sufficiently egregious to lose the Act's protection, as the comments were not made directly to the employer, did not contain excessive profanity, and did not involve threats or physically intimidating conduct.[37]

Inappropriate photos posted on employees' private Facebook pages also account for a large number of employment disputes.[38] Whether the photos are of cheerleaders drawing swastikas on the face of an inebriated peer at a social event, nursing home employees with their patients, or a high school teacher drinking alcohol on vacation,[39] stories of termination are abundant. Such photos can be detrimental to the employment of the individuals who post them on social media, as photographs fall outside the reach of the National Labor Relations Act.[40] This lack of statutory protection, coupled with the at-will nature of most employment agreements, often leaves individuals who have been terminated due to a controversial photo without remedy.

B. University Social Media Monitoring

In 2011, the National Collegiate Athletic Association ("NCAA") reported that Divisions I and II colleges and universities in the United States provided more than $2 billion in athletic scholarships to over 126,000 student-athletes.[41] Given this exorbitant sum, it is unsurprising that colleges and universities keep a close eye on their athletes' social media usage. One means of doing so is through third-party social media monitors who, for a fee, design customized search engines to scour each social media website for public social media posts that include words or

[36] *Id.*

[37] *Id.*

[38] *See, e.g.*, Neetzan Zimmerman, *Happy Now?: 'Good Employee' Lindsey Stone Fired Over Facebook Photo*, GAWKER (Nov. 22, 2012, 4:05 PM), http://gawker.com/5962796/happy-now-good-employee-lindsey-stone-fired-over-facebook-photo (posting a photo of employee jokingly displaying disrespect for the Tomb of the Unknown Soldier led to her termination from employment).

[39] Kaitlin Madden, *12 Ways to Get Fired for Facebook*, CAREERBUILDER.COM (Apr. 4, 2011, 5:39 PM), http://www.careerbuilder.com/Article/CB-1702-Workplace-Issues-12-Ways-to-Get-Fired-for-Facebook.

[40] *See, e.g.*, Karl Knauz Motors, Inc., No. 13-CA-46452, 2011 WL 4499437 (N.L.R.B. Div. of Judges Sept. 28, 2011) (holding that a photograph, unrelated to employment, was not protected).

[41] *Athletics Scholarships*, NAT'L COLLEGIATE ATHLETIC ASS'N (June 21, 2011), http://www.ncaa.org/wps/wcm/connect/public/NCAA/Resources/Behind+the+Blue+Disk/How+Do+Athletic+Scholarships+Work.

phrases that are pre-identified by the university.[42] Any "problems" uncovered by the search triggers an automatic email or text message to staff members at the college or university.[43] Examples of "flagged terms" requested by the University of Kentucky of its social media tracker include "payoff," "alcohol," "cheat sheet," "gay," "white power," "rape," "KKK," "Nazi," and "fight," among others.[44]

Universities maintain that the practice is necessary to preserve the reputation of the school, as well as to prevent young athletes from posting content they may later regret.[45] One University of Texas spokesman asserted, "[w]e're not out there to prevent anyone from being engaged in social media, but we want to make sure they understand what's going in [sic] social media and for them to be careful and to learn from their experience."[46] The desire of many college athletes to obtain as many "followers" or "friends" as possible,[47] leads to a heightened risk that athletes' social media posts or photos could potentially damage their own reputation or that of the school. Although NCAA officials believe that collegiate athletics departments are not allowed to ignore social media, they assert no intention to require student-athletes to provide username and password information.[48]

Primary criticisms of this common practice are not only constitutionally based, but also based on the fact that each university can customize its "red flag" words.[49] Some also note that it could lead to immense civil liability if a higher education institution were to detect and ignore a potential threat which subsequently led to an illegal act, such as murder.[50] The use of

---

[42] *See, e.g.*, *Other Products*, JUMPFORWARD, http://www.jumpforward.com/other-products (last visited Apr. 8, 2014).

[43] *Id.*

[44] Robert Shibley, *Did Somebody Say 'Gazongas'? You're Busted!*, FOUND. FOR INDIVIDUAL RIGHTS IN EDUC. (Aug. 22, 2012), http://thefire.org/article/14793.html.

[45] Jody Serrano, *Universities Might Have to Limit Monitoring, Set Social Media Policies in Stone under Proposal*, STATESMAN.COM (Feb. 10, 2013, 5:08 PM), http://www.statesman.com/news/news/local-education/universities-might-have-to-limit-monitoring-set-so/nWLNg.

[46] *Id.* (internal quotation marks omitted).

[47] Allie Grasgreen, *Watch What You Tweet*, INSIDE HIGHER ED (Aug. 27, 2012), http://www.insidehighered.com/news/2012/08/27/california-second-state-forbid-colleges-social-media-monitoring-athletes.

[48] Serrano, *supra* note 45.

[49] John Browning, *Universities Monitoring Social Media Accounts of Student-Athletes: A Recipe for Disaster*, 75 TEX. B.J. 840, 842 (2012).

[50] *Id.*

social media monitoring services has been banned in Arkansas, Delaware, California, Michigan, New Jersey, and Utah, but is still widely practiced in other states.[51]

In addition to social media monitoring services, some colleges in the U.S. require student-athletes to "friend" coaches or compliance officers, which provides such persons access to "friends-only" posts and photos.[52] Forced-friending is less intrusive than logging into an individual's account, as it does not provide access to the student's private Facebook messages. However, the practice is nonetheless subject to scrutiny. Critics claim that requiring student-athletes to "friend" a coach as a prerequisite to achieving membership on a team is commensurate with "requir[ing] athletes to bug their off-campus apartments."[53]

One well-known incident of student discipline resulting from online content arose in 2010, when a University of North Carolina football player, Marvin Austin, posted on Twitter regarding certain expensive purchases made on his account.[54] Following an NCAA investigation, Marvin was dismissed for violating NCAA agent benefits and ethical treatment rules.[55] This highly embarrassing incident is one factor that prompted the University to adopt a social media policy in which each student-athlete is required to "friend" a coach.[56]

---

[51] Bradley Shear, *Arkansas Bans NCAA Student-Athlete Social Media Monitoring Companies*, SHEAR ON SOC. MEDIA LAW (Apr. 8, 2013), http://www.shearsocialmedia.com//2013/04/arkansas-bans-ncaa-student-athlete.html.

[52] Bob Sullivan, *Govt. Agencies, Colleges Demand Applicants' Facebook Passwords*, NBC NEWS (Mar. 6, 2012, 6:13 AM), http://redtape.nbcnews.com/_news/2012/03/06/10585353-govt-agencies-colleges-demand-applicants-facebook-passwords.

[53] *Id.*

[54] *Id.*

[55] Justin Eisenband, *North Carolina Tarheels Scandal: Marvin Austin and Co. Suspended for Entire Year*, BLEACHER REPORT (Oct. 11, 2010), http://bleacherreport.com/articles/488187-north-carolina-scandal-austin-quinn-little-all-suspended-for-season.

[56] Sullivan, *supra* note 52; *see* UNIV. OF N.C., THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL DEPARTMENT OF ATHLETICS POLICY ON STUDENT-ATHLETE SOCIAL NETWORKING AND MEDIA USE (Apr. 2012), *available at* http://www.goheels.com/fls/3350/pdf/Compliance/SocialNetworkingPolicy.pdf?SPID=111196&DB_OEM_ID=3350.

IV. PROBLEMS CONTEMPLATED BY SNOPA

As noted, SNOPA prevents employers, higher education institutions, and public elementary and secondary schools from requiring employees, potential employees, or students to disclose usernames and passwords for their respective private social media sites.[57] It also prevents disclosure by such individuals of his or her private email account.[58] In doing so, SNOPA contemplates some issues that have been arising with regard to job applicants being asked to disclose social media login information.[59] However, while SNOPA does prevent schools from requesting or requiring login information from students, it does not address the more common disputes that arise out of the use of social media monitoring sites by colleges and universities.[60]

A. Employers Requesting Candidates Username & Password

One case arose in 2010, sparking legislation in Maryland, when a former Maryland corrections officer, Robert Collins, after taking a leave of absence, sought to be reinstated to his former position.[61] Collins' former employer requested that he provide his Facebook username and password, and indicated to him that doing so was a condition of recertification.[62] After Collins reluctantly complied, the employer began searching through Collins' messages, wall posts, and photos "to make sure [he was] not a gang member or [had] any gang affiliation."[63] The ACLU complained about the practice of this particular agency, and the agency subsequently amended its policy to ask candidates to instead log in during interviews.[64]

---

[57] Social Networking Online Protection Act, H.R. 537, 113th Cong. § 2(a) (2013).

[58] *Id.*

[59] *See* discussion *infra* Part IV.A.

[60] *See* H.R. 537; *see also* discussion *supra* Part III.B.

[61] *Resume, Cover Letter And Your Facebook Password?*, NPR (Mar. 21, 2012), *available at* http://www.npr.org/2012/03/21/149091139/resume-cover-letter-and-your-facebook-password.

[62] Doug Gross, *ACLU: Facebook Password Isn't Your Boss' Business*, CNN TECH (Mar. 22, 2012, 5:54 PM), http://www.cnn.com/2012/03/22/tech/social-media/facebook-password-employers.

[63] *Id.*

[64] Shannon McFarland & Manuel Valdes, *If You Want A Job, You May Have To Turn Over Your Facebook Password*, BUS. INSIDER (Mar. 21, 2012),

Numerous other cases have arisen in recent years throughout various jurisdictions, relevant to the issues contemplated by SNOPA. One New York City statistician, Justin Bassett, was asked for his Facebook username and password during a job interview; he refused and subsequently withdrew his application based on principle.[65] On another occasion, an elementary school teacher's aide, Kimberly Hester, posted an inappropriate photo of a co-worker with her pants around her ankles, and a parent of the student reported her to the school.[66] The school superintendent requested three times that she provide him with her Facebook password, and each time, Hester declined to do so.[67] Hester was subsequently terminated from her full-time position.[68]

While requesting a password from a job candidate is increasingly more common among employers, it is more prevalent among public agencies, namely, law enforcement or 911 dispatchers.[69] The practice is defended by many, who assert that in conducting background investigations, an individual's social media content is far more indicative of his or her character than inquiring with friends and neighbors of the individual.[70] Among the category of content that would trigger an alarm are derogatory behavior, "inappropriate pictures or relationships with people who are underage, [and] illegal behavior."[71]

B. Education Institutions

Currently, states are also responsible for legislation regulating social media tracking services discussed *supra*, and SNOPA will not change this.[72] In addition to bans on requests from employers, SNOPA would prevent higher education institutions, as well as elementary and secondary education institutions, from

http://articles.businessinsider.com/2012-03-21/news/31217978_1_facebook-password-social-networking-interviewer.

[65] *Id.*

[66] Helen A.S. Popkin, *Failing to Provide Facebook Password Gets Teacher's Aide Fired*, NBC NEWS (Apr. 3, 2012, 3:04 PM), http://sys03-public.nbcnews.com/technology/failing-provide-facebook-password-gets-teachers-aide-fired-642699.

[67] *Id.*

[68] *Id.*

[69] McFarland & Valdes, *supra* note 64.

[70] *Id.*

[71] *Id.*

[72] *See* H.R. 537, 113th Cong. (2013) (containing no express federal preemption clause); Shear, *supra* note 51 (listing the states that have enacted legislation banning the use of social media monitoring firms by schools).

requesting access to students' social media accounts or private email accounts.[73]

In 2007, a Mississippi high school cheerleading coach required each member of the team to reveal passwords to their Facebook accounts.[74] The coach subsequently logged onto one particular cheerleader's Facebook page, retrieved private messages between the cheerleader and a fellow student, and disseminated them to other cheerleading coaches, teachers, the principal, and the superintendent.[75] The messages contained a great deal of profanity.[76] By distributing the private messages, the coach not only publically humiliated the student, but she subsequently deprived her of the opportunity to compete in a cheerleading competition.[77] The student filed suit, alleging a violation of her right to privacy and First Amendment rights.[78]

V. WHY ARE PROBLEMS CONTEMPLATED BY SNOPA, PROBLEMS?

A. Fourth Amendment

The Fourth Amendment to the U.S. Constitution protects individuals against unreasonable search and seizure,[79] and more broadly, vests in Americans the right to privacy.[80] Although historically applied to search of an individual's home or vehicle, the protection has been extended to electronic channels as well. Courts have held that individuals are entitled to the same reasonable expectation of privacy to their email accounts as they are to conventional written letters.[81]

In *R.S. ex rel. S.S. v. Minnewaska Area School District*, a

[73] H.R. 537.

[74] Brian Stewart, *Student Files Lawsuit After Coach Distributed Private Facebook Content*, STUDENT PRESS L. CENTER (July 22, 2009), http://www.splc.org/news/newsflash.asp?id=1938.

[75] *Id.*

[76] Brian Kumnick, *Student Sues Over Coach Accessing Her Facebook Account*, FINDLAW (Aug. 3, 2009, 11:50 AM), http://blogs.findlaw.com/injured/2009/08/student-sues-over-coach-accessing-her-facebook-account.html.

[77] *Id.*

[78] *Id.*

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

[80] *Your Right to Privacy*, ACLU (July 17, 2003), http://www.aclu.org/technology-and-liberty/your-right-privacy.

[81] R.S. *ex rel.* S.S. v. Minnewaska Area Sch. Dist., 894 F.Supp.2d 1128, 1142 (D. Minn. 2012) (citing United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008)).

middle school student, after posting a comment on Facebook about a school hall monitor, was forced to provide her username and password to school officials, who searched her Facebook account, including private messages.[82] The court held that since at least some of the messages and information accessed by the school were in the student's sole possession and protected by her password, the school violated her Fourth Amendment reasonable expectation of privacy.[83] In reaching its decision, the court reasoned that since the student's activity occurred off of school grounds, the school did not meet the U.S. Supreme Court's criterion of a "'substantial interest of teachers and administrators in maintaining discipline *in the classroom and on school grounds*.'"[84] Moreover, it noted that the school officials lacked reasonable grounds to suspect that a search of the student's Facebook account would uncover evidence that the student violated the law or rules of the school.[85] Thus, the student had a reasonable expectation of privacy to private information on her Facebook account.[86]

The aforementioned case is just one illustration of how a school administrator or employer requiring his or her subordinates to provide usernames and passwords to social media sites can be a severe infringement on the individual's Fourth Amendment rights. The risk is heightened by the fact that an array of information can be discovered through a search of one site alone. However, Fourth Amendment protections do not encompass all content available on Facebook. One court held that Facebook users, who post publicly available comments or photos, are not entitled to a reasonable expectation of privacy.[87] It reasoned that when creating a Facebook account and consenting to the terms of use, which state that personal information can be shared with others, the plaintiff knew that her information might be publically available, and was barred from claiming that she had Fourth Amendment protection.[88]

---

[82] *Id.* at 1133–34.

[83] *Id.* at 1142, 1147.

[84] *Id.* at 1143 (quoting New Jersey v. T.L.O., 469 U.S. 325, 336–37 (1985) (emphasis added)).

[85] *Id.* at 1143.

[86] *Id.* at 1142.

[87] *See* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 656–57 (N.Y. Sup. Ct. 2010).

[88] *Id.*

B. First Amendment

The First Amendment of the U.S. Constitution protects the individual right of religious freedom, speech, and press.[89] However, this right is not afforded without limits. When individual speech constitutes, for example, a true threat, defamatory statement, or obscenity, it is not protected by the First Amendment.[90]

While private employment disputes regarding free speech are analyzed under the protected concerted speech framework,[91] the speech of students is scrutinized under the First Amendment. Although students are entitled to constitutional protections while on school property, the school is allowed to restrict speech, even if it is protected speech, outside of school.[92] A school cannot prevent a student from making certain speech simply because it is controversial, but such restrictions are warranted when "the school . . . [has] a good reason to believe that [a student's] expression will disrupt school or infringe on the rights of others."[93] When students utilize school computers and Internet, officials are entitled to monitor the students' online activity.[94] Conversely, schools cannot discipline students for posting content online during non-school hours, using a non-school Internet connection and non-school computer, and using a non-school email, unless such content constitutes a true threat, defamatory statement, or obscenity.[95] In such a case, the student could be investigated by the police, and the school could be notified of the student's activity.[96] Moreover, schools can punish students for posting evidence that they violated school rules in some manner, such as skipping class.[97]

A case arising in Florida, *Evans v. Bayer* dealt with a high school senior who created a Facebook group entitled, "Ms. Sarah Phelps is the worst teacher I've ever met," the purpose of which

---

89 U.S. CONST. amend. I.

90 *Student Rights and Responsibilities in the Digital Age: A Guide for Public School Students in Washington State*, ACLU WASH. ST. (Jan. 2012), http://aclu-wa.org/student-rights-and-responsibilities-digital-age-guide-public-school-students-washington-state#IA.

91 *See supra* Part II.

92 ACLU WASH. ST., *supra* note 90.

93 *Id.*

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.*

was to allow students to comment on their dislike for the particular teacher.[98] The group page included a photo of the teacher.[99] The court held that because the speech was non-violent, non-threatening, and made off-campus, it did not undermine the values of a school education, and was therefore entitled to First Amendment protection.[100]

Another case arose when a high school student created a parody MySpace[101] profile (another popular social networking site) for his school principal.[102] On the profile he made several references to the principal's sexual orientation, use of marijuana, excessive drinking, and pill taking, among other things.[103] The student was reported and subsequently punished by the school for his conduct.[104] The court ultimately held that because the website was created using a private computer off of school grounds, and did not cause a disruption in school, that it was protected speech.[105]

C. Due Process Right to Privacy

The Fifth and Fourteenth Amendments to the U.S. Constitution prohibit the deprivation of "life, liberty, or property, without due process of law."[106] Courts have interpreted "due process" to apply not only to procedural matters, but also substantive liberties, including the right to privacy.[107] In the landmark case *Griswold v. Connecticut*,[108] the Supreme Court noted that the Fifth Amendment provided "protection against all government invasions 'of the sanctity of . . . the privacies of life.'"[109] This right to privacy includes not only freedom from bodily restraint, but the freedom to "engage in any of the common

98 Evans v. Bayer, 684 F.Supp.2d 1365, 1367 (S.D. Fla. 2010).

99 *Id.*

100 *Id.* at 1374.

101 MYSPACE, https://myspace.com (last visited Apr. 23, 2014).

102 Layshock *ex rel.* Layshock v. Hermitage Sch. Dist., 650 F.3d 205, 207–08 (3d Cir. 2011).

103 *Id.* at 208.

104 *Id.* at 207, 210.

105 *Id.* at 219.

106 U.S. CONST. amend. V; *see also* U.S. CONST. amend. XIV § 1.

107 James W. Ely, Jr., *Due Process Clause*, THE HERITAGE GUIDE TO THE CONSTITUTION, http://www.heritage.org/constitution/#!/amendments/14/essays/170/due-process-clause (last visited Apr. 23, 2014).

108 381 U.S. 479 (1965).

109 *Id.* at 484 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

occupations of life," such as raising children, worshiping freely, and acquiring knowledge.[110] Essentially, the right to privacy in the Fifth and Fourteenth Amendments is the right to be left alone and the right to enjoyment of life.[111]

It is clear how this right to privacy may be implicated in the context of social media activity. Individuals have the right to communicate, share information, and connect with others free of intrusion, and a mandatory username and password disclosure could be considered a severe infringement on the individual's right to be left alone and conduct daily life as he or she sees fit.

D. Undue Pressure on Employees or Potential Employees

Although providing social media login information is not *required* of employees or applicants,[112] simply by the nature of the request, such individuals are likely placed under extreme pressure to consent. Job cuts and overall career outsourcing in certain industries, coupled with a relatively high unemployment rate (exceeding 7% in 2013)[113] creates an atmosphere providing very little bargaining power for employees in terms of gaining and maintaining employment. It is suggested that such fear and pressure is a primary cause of employees' or prospective employees' submission to interviewers' or employers' requests for social media login information.[114] The director of policy and advocacy at the Privacy Rights Clearinghouse stated, "If you feel most of the other applicants are going to be providing this information, you're probably not going to be willing to say no."[115] Moreover, by being asked, job applicants might assume that it is common practice for applicants to provide such information and that he or she is expected to.

---

110 Meyer v. Nebraska, 262 U.S. 390, 399 (1923).

111 *Development of the Right to Privacy*, JUSTIA U.S. LAW, http://law.justia.com/constitution/us/amendment-14/30-right-of-privacy.html (last visited Apr. 23, 2014).

112 *See* Sullivan, *supra* note 52 (highlighting that five of the eighty employees hired in the last three hiring cycles by the Maryland Department of Corrections did not provide access to their social media accounts).

113 *News Release: The Employment Situation – February 2014*, U.S. DEP'T OF LABOR BUREAU OF LABOR STATISTICS (Mar. 7, 2014, 8:30 AM), *available at* http://www.bls.gov/news.release/pdf/empsit.pdf.

114 Martha C. White, *Can Interviewers Insist on 'Shoulder Surfing' Your Facebook Page*?, TIME (Mar. 9, 2012), http://business.time.com/2012/03/09/can-interviewers-insist-on-shoulder-surfing-your-facebook-page.

115 *Id.*

The compelled speech doctrine established in *West Virginia v. Barnette Board of Education*[116] may be applicable in situations where an employer requires an employee to provide a social media username or password. In that landmark case, the U.S. Supreme Court held that a state law forcing elementary school students to salute the U.S. flag and recite the pledge of allegiance was unconstitutional.[117] Requiring disclosure of social media usernames and passwords could essentially be viewed as compelling employees, job applications, or students to act. However, such mandatory disclosures likely do not fit within the realm of *Barnette*'s intended protections. Refusing to provide access to social media information is not akin to forcing students to confess their faith and allegiance to their country.[118] While the latter obliges individuals to assert a particular position or belief, the former simply provides access to information or beliefs that an individual has already expressed through social media. The "speech" itself is the disclosure of login information, not the information that can be accessed after using the login information. Therefore, the practice by employers or school administrators of obtaining social media login information is likely not prohibited by the compelled speech doctrine.

However, once an interviewer receives the login information, he or she has gained access to a plethora of information about the candidate which he or she potentially cannot legally inquire into in an interview.[119] Employers violate federal law when refusing to hire, or in discharging an individual based on religion, race, color, sex, or national origin.[120] Thus, interview questions relating to the same are prohibited.[121] However, the employer can readily determine such information through even a brief search of an individual's Facebook account, through the individual's profile information, or even photos and posts. Requesting login information in some states is thus a potentially legal means to achieve an illegal purpose of discriminating against the

116 319 U.S. 624, 642 (1943).

117 *Id.*

118 *See id.* (stating that the constitution protects individuals' personal beliefs and faith).

119 *See* White, *supra* note 114 (describing how employers can have prospective employees scroll through their "friends only" posts).

120 *See* 42 U.S.C. § 2000e-2 (1991).

121 *See* Christina Couch, *8 Illegal Interview Questions to Avoid*, BANKRATE.COM (Nov. 27, 2012), http://www.bankrate.com/finance/jobs-careers/illegal-interview-questions.aspx#slide=1.

individual.

VI. STATE REGULATION

Effective October 1, 2012, Maryland became the first state to prohibit employers from requiring employees to disclose social media login information.[122] In recognition of the ubiquitous presence of social media, lawmakers responded by passing the law, which promises to limit employers' ability to monitor employees' online activity, and "'creates a bright line as to what employers can and can't do.'"[123]

Effective January 1, 2013, the Illinois Right to Privacy in the Workplace Act was amended, making it illegal for an employer to request any employee or prospective employee to provide his or her password or other related information, in order for the employer to gain access to his or her social networking account.[124] The amendment also prohibits employers from demanding access in any manner to such accounts or profiles.[125] Moreover, employers are prohibited from using Electronic Employment Verification Systems without providing ample notice to employees or prospective employees.[126]

Both Maryland's and Illinois's decisions to pass laws banning the practice of many employers was highly influenced by Robert Collins' story, discussed *supra*.[127] Maryland and Illinois are just two of the multiple states in the U.S. that have passed legislation prohibiting the request for social media usernames and passwords by employers, potential employers, and schools. Other states have also followed suit, passing similar legislation, including California[128] and Delaware,[129] among others.

---

122 Catherine Ho, *Maryland Becomes First State to Prohibit Employers from Asking for Facebook Logins*, CAPITAL BUS. BLOG (May 3, 2012, 1:15 PM), http://www.washingtonpost.com/blogs/capital-business/post/maryland-becomes-first-state-to-prohibit-employers-from-asking-for-facebook-logins/2012/05/03/gIQAsE1GzT_blog.html.

123 *Id.*

124 Revisions to the *Right to Privacy in the Workplace Act*, LEGAL DIVISION: RIGHT TO PRIVACY ACT WITHIN THE WORKPLACE, http://www.illinois.gov/idol/Laws-Rules/legal/Pages/privacy-workplace.aspx (last visited April 8, 2014).

125 *Id.*

126 820 ILL. COMP. STAT. ANN. 55/12 (West 2014).

127 Chad Bascombe, *Illinois Facebook Law Bans Employers From Violating Your Privacy*, POLICYMIC (Aug. 15, 2012), http://www.policymic.com/articles/12680/illinois-facebook-law-bans-employers-from-violating-your-privacy.

128 CAL. LAB. CODE § 980 (West 2014).

129 DEL. CODE ANN. tit. 14, § 8103 (West 2014).

VII.INADEQUACY OF SNOPA

Having highlighted two of the numerous issues that arise in the context of social media, Facebook firing and higher institution social media monitoring, the issue to be addressed is whether SNOPA will mitigate or prevent such disputes. In short, the answer is undeniably, no. As discussed *supra*, SNOPA only prohibits certain entities from requesting or compelling the disclosure of social media or private email passwords, and prohibits subsequent discrimination or discipline for the failure to do so.[130]

As a preliminary analysis, the various social media challenges discussed herein clearly should be regulated at the federal level. First, since Facebook knows no territorial boundaries, legislation that regulates the utilization of Facebook activity and content should similarly not be constricted by state lines. Second, regulating at the state level creates great inequities. It is wholly unfair to require a job applicant for a multi-state company to provide a user name and password, while relieving another job applicant to the same company of this responsibility simply because he or she seeks to gain employment with the company in a different state. However, SNOPA was very narrowly constructed to prevent employers or higher education institutions from requiring employees, prospective employees, or students to provide them with his or her *username* or *password*.[131] A survey conducted in June of 2012 of 1,000 high level private company executives, corporate counsel, and human resource professionals, revealed that 1% of respondents requested social media logins during the hiring process.[132] While such a survey is not determinative, it does highlight a very important point: perhaps all of the hype is unfounded.

Despite commonplace employment disputes arising from employers discharging employees based on public information obtained from employees' Facebook accounts, SNOPA will not actually stymie such suits or in any significant way alleviate those types of issues. If SNOPA is enacted, employers can still gain access to employees' Facebook information by "friending" employees, and can still view any publicly available content. This latter risk is amplified by the fact that a large number of

130 H.R. 537, 113th Cong. (2013).
131 *Id.*
132 Bascombe, *supra* note 127.

Facebook users do not adequately utilize privacy settings to prevent discovery of potentially incriminating photos or posts.[133] Additionally, SNOPA does not contemplate university athletic departments' social media policies.[134] The Act is silent on employers or higher education institutions obtaining publicly available information from employees' or students' Facebook accounts, and using it as a ground for discharge or expulsion.[135] Moreover, SNOPA does not encompass the tremendous problem of social media monitoring systems.

Furthermore, regardless of a prohibition under SNOPA, employers who engage in the questionable practice might be engaged in illegal conduct anyway under the Stored Communications Act.[136] This legislation prohibits individuals from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . or intentionally exceed[ing] an authorization to access that facility."[137] The application of the Stored Communications Act has been limited by courts to information on social media sites that can only be viewed with the user's permission, such as private messages or photos blocked by privacy settings.[138] In many situations, by providing the interviewer with a Facebook username and password, the applicant is not actually authorizing access, as he or she may feel *compelled* to disclose the information.[139]

---

133 *See* Courteney Palis, *Facebook Privacy Options Ignored By Millions Of Users: Consumer Reports*, HUFFINGTON POST (May 3, 2012, 11:54 AM), http://www.huffingtonpost.com/2012/05/03/facebook-privacy-consumer-reports_n_1473920.html (reporting that in 2011, 28% of Facebook users were sharing almost all, if not all of their posts with users who were not included in their group of "friends").

134 H.R. 537.

135 *Id.*

136 Joanna Stern, *Demanding Facebook Passwords May Break Law, Say Senators*, ABC NEWS (Mar. 26, 2012), http://abcnews.go.com/Technology/facebook-passwords-employers-schools-demand-access-facebook-senators/story?id=16005565.

137 18 U.S.C. § 2701 (2012).

138 Nicholas D. Beadle, Note, *A Risk Not Worth the Reward: The Stored Communications Act and Employers' Collection of Employees' and Job Applicants' Social Networking Passwords*, 1 AM. U. BUS. L. REV. 397, 400 (2012).

139 *Id.* at 404.

VIII. PRACTICE WORTHY OF CONDEMNATION?

Criticisms against some companies' or schools' social media policies often overlook the benefits of such practices. The significance and essentiality of the right to privacy, for the most part, cannot be disputed. However, one could argue, as this note does, that certain types of employees or students, who are held to a higher standard in society, should also be held to a higher standard in their online activity. The nature and sensitivity of the particular profession, as well as job duties, should be considered. Crude, provocative, or otherwise inappropriate online posts or photos may be unacceptable from an attorney, for instance, whereas overlooked or tolerated from a bartender.

Since public officers are scrutinized more intensely than others, for valid reasons, why should officers' social media accounts be exempt from the scrutiny? For instance, if a man or woman responsible for the safety and well-being of a community were a racist, drug addict, pedophile, or had any other affiliation, trait, or bias that could potentially endanger society, and searching through the individual's Facebook account were the sole mean by which that fact could be revealed, shouldn't such a search be *condoned*, rather than *condemned*? Robert Collins' incident with the Maryland Department of Corrections received great media attention, shunning the practice of searching through an applicant's Facebook page outright.[140] However, a spokesperson of the Department reported to the ACLU that out of the 2,689 applicants whose social media pages it reviewed, it denied employment to seven of them.[141] The basis for denial was that these seven applicants' pages contained photos of them flashing commonly known gang symbols.[142] All steps should be taken to ensure that prison guards have no gang affiliation, as it could create a conflict of interest and severely affect his or her ability to adequately serve the position. If searching through a Facebook page is an effective way to do so, it should be permitted.

Teachers, namely middle or secondary school teachers, are another group of employees within the realm of those who should be required to undergo a private Facebook content search.

140 *See supra* Part IV.A.
141 Sullivan, *supra* note 52.
142 *Id.*

Teachers spend roughly one-fourth of each weekday with the country's growing youth and are responsible for educating this population.[143] Thus, teachers have a heightened duty to project the utmost class, integrity, and responsibility. This is especially true among young teachers, whom students would be most likely to relate to and admire. Teachers who post inappropriate content on Facebook, that their students are exposed to, not only severely undermine their authority as educators and leaders of classes, but also glorify or approve of such behavior.

Moreover, there exists no fundamental right to play college sports. Colleges and universities invest a great deal of time and money building athletics programs, recruiting athletes, providing scholarships, etc.[144] Since obtaining a place on an athletic team is viewed by many as a privilege, it may not be so appalling that directors place restrictions on such a privilege. The contention that monitoring a student-athlete's social media activity is the same as bugging his or her non-school rented apartment[145] is slightly dramatic, as these critics completely overlook the fact that Facebook posts are not private. The purpose of social media is to provide an outlet to connect with other individuals in a leisurely manner. It is completely voluntary, and allows students to voice personal opinions if they so choose. By "friending" a student, officials are exposed to information about the student that other "friends" of the student are also exposed to, which is vastly different from obtaining private information about the student. Had the University of North Carolina officials not discovered Marvin Austin's Twitter post,[146] the school would not have known that the student-athlete was violating several NCAA rules, rendering him ineligible to play football. Lest we forget, this was a *public* post, not a private message or email.

Essentially, student-athletes who receive scholarships to

143 *See* Marga Mikulecky, *Number of Instructional Days/Hours in the School Year*, EDUC. COMM'N OF THE STATES 1–8 (Mar. 15, 2013), *available at* http://www.ecs.org/clearinghouse/01/06/68/10668.pdf (providing a brief overview of each state's schooling requirements).

144 *See* Alicia Jessop, *The Economics of College Football: A Look at the Top-25 Teams' Revenues and Expenses*, FORBES.COM (Aug. 31, 2013, 10:32 AM), http://www.forbes.com/sites/aliciajessop/2013/08/31/the-economics-of-college-football-a-look-at-the-top-25-teams-revenues-and-expenses (providing a chart that details the amount of money spent by the nation's most prominent collegiate football programs).

145 Sullivan, *supra* note 52.

146 *See supra* Part III.B.

participate in collegiate sports have formed an agreement.[147] In exchange for free tuition, the athlete agrees to represent the school well through his or her athletic ability, as well as character. Due to the privileged nature of the agreement, these students should be held to a higher standard than students who are not awarded athletic scholarships. Student-athletes who are provided an extremely rare and extraordinary opportunity to participate in a college sport (especially those on scholarship), *should be* monitored and held accountable for online "bragging" about violating the rules of their contracts, as well as other explicit and inappropriate content that casts serious doubt on character and reliability. Thus, social media monitoring is an effective and appropriate practice in order to ensure that student-athletes are complying with the rules of their respective programs.

XI. CONCLUSION

The practice contemplated by SNOPA should not be outright condemned or condoned. While the power to search through employees' Facebook pages can render such individuals vulnerable to discrimination and abuse, it also has highly probative value. Law enforcement agencies and primary and secondary education institutions *should* be browsing the social media content of applicants. It was proper for Robert Collins to provide his username and password on his reinstatement interview. Law enforcement individuals hold a great deal of power over average citizens, so the hiring process in law enforcement should be extensive and perhaps even intrusive. Not only are law enforcement officers given weapons to use at their discretion to carry out job responsibilities, but they can, for instance, conduct arrests, as well as search through individuals' automobiles and homes. With this heightened authority comes

147 *See, e.g.*, Ross v. Creighton Univ., 957 F.2d 410, 416 (7th Cir. 1992) ("It is held generally in the United States that the 'basic legal relation between a student and a private university is contractual in nature. The catalogues, bulletins, circulars, and regulations of the institution made available to the matriculant become a part of the contract.'" (quoting Zumbrun v. Univ. of S. Cal., 101 Cal. Rptr. 499, 504 (Cal. Ct. App. 1972))); Taylor v. Wake Forest Univ., 191 S.E.2d 379, 382 (N.C. Ct. App. 1972) ("[Plaintiff], in consideration of the scholarship award, agreed to maintain his athletic eligibility and this meant both physically and scholastically . . . Participation in and attendance at practice were required to maintain his physical eligibility. When he refused to do so . . . he was not complying with his contractual obligations.").

heightened responsibility. The persons in charge of hiring law enforcement officers should take every step necessary to ensure that he or she is completely free from any bias toward the subject matter of the position that may affect his or her ability to adequately conduct duties. The rationale employed by Robert Collins' supervisor in searching through his Facebook page was to verify that he had no gang affiliation.[148] If the Department did not conduct the search and Collins did in fact have a gang affiliation, reinstating him to his position as a corrections officer could be extremely dangerous. A potential conflict of interest could not only jeopardize the safety of other officers, but also other inmates and the public as a whole. Provided that the search truly is tailored toward discovering content that could cast doubt upon the applicant's ability to conduct the job properly and effectively, requesting login information to social media accounts should be a valid means to achieve the goal of ensuring that the most qualified law enforcement officers are employed. Similarly, teachers have a duty to ensure that they are educating students properly, both inside and outside of the classroom. A high burden is placed on primary and secondary teachers to not only teach the students, but also to project a high moral compass, instilling in our youth wholesome values. If the individual teacher does not display positive qualities on social media, how can he or she encourage the students to?

Students, on the other hand, should not be required to provide login information for social media sites. When applying to college, applicants do not receive the same level of scrutiny as individuals applying for law enforcement or teaching positions, for instance. Students are not responsible for the well-being of others and are not given heightened duties. By gaining acceptance to a college or university, students essentially just gain the right to attend the particular school. Unlike the potential host of information that could be uncovered from searching a law enforcement officer's Facebook page, it is highly unlikely that searching through private information on a student's Facebook page would reveal any damaging information that would severely undermine the student's ability to attend the school.

On the other hand, the practice by colleges and universities of utilizing outside services in order to monitor the *public* social media activity of student-athletes is warranted. Social media

148 Gross, *supra* note 62.

monitoring is not prohibited by SNOPA, nor should it be. It is not nearly as troublesome as requiring access to the student's *private* online content, like login information to social media accounts and passwords to private email accounts. These athletes are subject to discipline if posts or photos prove that they are engaged in illegal activity or violating the rules of their contracts. Keeping a watchful eye for such information is far from an invasion of privacy or a deprivation of the students' constitutional rights.

The broader and more prevalent issue of "Facebook firing" might be better served if employees or potential employees simply stopped placing inappropriate photos and posts on the Internet. Another alternative is for the individual to ensure that his or her social media account privacy settings are set accordingly so photos and posts remain private.

SNOPA is both over-inclusive and under-inclusive. The conduct that SNOPA prevents does not occur frequently or on a sufficiently large scale to constitute a substantial problem. It is over-inclusive because there are certain situations in which investigating a job applicant's private social media information is crucial to ensure that an individual is qualified for the position, and free from bias or inappropriate affiliations. It is under-inclusive because it does not encompass a prevalent problem of "Facebook firing" caused by social media use. A multitude of issues arise when employees' or students' public social media content is discovered by employers or schools, and subsequently employed as a ground for termination or discipline. However, SNOPA will have no bearing on access to public posts or photos. In sum, if passed, SNOPA likely will have little to no impact on the foremost issues.