Hamline University's School of Law's Journal of Public Law and Policy

Volume 35
Issue 1 *Transcending Intellectual Property Rights: An Exploration Into the Unchartered Territories of the Intangible, Infringed, and the Internet*

Article 3

2-26-2014

SNOPA and the PPA: Do You Know What It Means For You? If SNOPA (Social Networking Online Protection Act) Or PPA (Password Protection Act) Do Not Pass, The Snooping Could Cause You Trouble

Angela Goodrum

SNOPA AND THE PPA: DO YOU KNOW WHAT IT MEANS FOR YOU?
IF SNOPA (SOCIAL NETWORKING ONLINE PROTECTION ACT) OR PPA (PASSWORD PROTECTION ACT) DO NOTPASS, THE SNOOPING COULD CAUSE YOU TROUBLE

*By Angela Goodrum**

I. INTRODUCTION

Social media has introduced a new world of opportunities for sharing, networking, staying in touch, and communicating. However, just as it has provided a vast medium for the exchange of information, it has also created ample opportunities for others, such as hiring personnel or admission offices to snoop around, discriminate, and base their hiring or admission decisions, in part, on an individual's online persona. While online personas are subject to searches from a variety of individuals or entities, such as organizations, churches, and potential or previous clients, this article will focus primarily on (i) potential employers; and (ii) educational institutions. The focus is narrow, because the outcomes of these entities' snooping practices have the greatest potential impact on our livelihood and opportunities for educational or career advancement. Therefore, this snooping could have employment or educational implications for a growing number of the population if the Social Networking Online Protection Act (SNOPA) or the PPA (Password Protection Act) is not passed into law.

Section II of this article defines social media and discusses its growing popularity. Then, section III will highlight the reality of fraud on the Internet and explain why it is a legitimate concern for applicants as there is no guarantee that the online searches the potential employer or educational institution conducts will return legitimate data. Also, it will explain the value of SNOPA and the PPA by revealing some of the inadequacies of existing privacy laws

which leave the American people vulnerable. This article demonstrates numerous issues that individuals have encountered with employers and schools as a result of the practice of snooping through social media. Section IV explores the reasons for advocating the passage of SNOPA and PPA and discusses alternative protection that maybe afforded under other laws. In conclusion, section V urges individuals to take action to prompt their local government to ensure its citizen's privacy rights are not squandered away. Lastly, argument will be made regarding the matters that individuals should consider if the laws do not fully provide coverage.

II. BACKGROUND

A. Social Media and Its Popularity

The National Labor Relations Board defines social media as "various online technology tools that enable people to communicate easily via the Internet to share information and resources."[1] Social media can include Facebook, Twitter, LinkedIn and other similar sites. Social media has become a part of many individuals' everyday lives, with many not going a day without using some form of social media.[2] These advancements in technology are reshaping

---

* J.D. Candidate 2015, Barry University Dwayne O. Andreas School of Law; B.A. (Criminal Justice), University of Central Florida, 2006. The author would like to thank her husband, Robert, and her mother for their unconditional love, support, and encouragement.

[1] OM 11-74. NLRB Office of the General Counsel, (January 2012); Leslie Hayes & Sally J. Cooley, *Social Media-Striking the Balance Between Employer and Employee*, 55-DEC ADVOCATE (IDAHO) 22, 22 (2012), *available at* http://isb.idaho.gov/pdf/advocate/issues/adv12novdec.pdf.

[2] Nathan J. Ebnet, Note, *It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening With The Fair Credit Reporting Act*, 97 MINN. L. REV. 306, 308 (2012) (discussing the popularity of social media has exploded over the last several years and millions are dedicated to the use of the sites); *see, e.g.*, Samantha L. Miller, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 544 (2008); Lindsay S. Feuer, Note, *Who is Poking Around Your Facebook*

human mechanisms for communication and social interaction at such a rapid pace that society generally fails to recognize or question the changes and their impacts.[3] Facebook is currently the leading social networking site and has garnered over 1 billion active users throughout the world.[4] To put it in perspective, if Facebook were a country, it would be the third largest in the world. Facebook as a country would be larger than the United States, only falling short of China and India.[5] Even when on the move, people have social media readily available and at their fingertips, with more than 604 million active users accessing Facebook via their mobile devices.[6]

Also steadily increasing in popularity is Twitter, which has reported receiving 1 billion "tweets" per week and 500 million users in 2012.[7] Another popular social media site is LinkedIn,

---

Profile?: The Need to Reform The Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites, 40 HOFSTRA L. REV. 473, 482 (discussing how everyday millions of people use Facebook to keep up with their friends).

[3] Langdon Winner, Essay on Technologies as a Form of Life (1977), http://hettingern.people.cofc.edu/Nature_Technology_and_Society_Fall_2010/Winner_Ttechnologies_as_Forms_of_Life.pdf (discussing the point that society fails to recognize the many ways that technology shapes the structure for human activity. "[T]echnologies are not merely aids to human activity, but also powerful forces acting to reshape that activity and its meaning." Langdon Winner promotes a theory of technological somnambulism whereby society willingly "sleepwalks" through the process of technological changes that significantly affect the "conditions of human existence.").

[4] 2013 Social Networking Websites Comparisons, Top Ten Review, http://social-networking-websites-review.toptenreviews.com/ (last visited Jan. 8, 2012); Facebook, Key Facts, http://newsroom.fb.com/Key-Facts (last visited May 15, 2013); s*ee also* Andy Kazeniac, *Social Networks: Facebook Takes Over Top Spot, Twitter Climbs*, COMPETE PULSE BLOG (Feb. 9, 2009), http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/.

[5] *See* Ebnet, *supra* note 2, at 316; Brian Solis, *Facebook Connects 500 Million People: Defines a New Era of Digital Society*, BRIANSOLIS.COM (July 22, 2010), http://www.briansolis.com/2010/07/facebook-connects-500-million-people-defining-a-new-era-of-digital-society/.

[6] Facebook, Key Facts, *supra* note 4.

[7] *Twitter*, WIKIPEDIA, http://en.wikipedia.org/wiki/Twitter, (last visited May 15, 2013); *Twitter Statistics*, KISSMETRICS BLOG, blog.kissmetrics.com/

which operates the world's largest professional network on the Internet with more than 74 million members in the United States as of January 9, 2013.[8] The fastest growing demographic reported on LinkedIn is students and recent college graduates, who make up 20 million of LinkedIn's members as of May 2012.[9]

Just as social networking sites are steadily growing in popularity with individuals, so too, is the popularity increasing with businesses for the purposes of using it as a screening tool.[10] In 2011, the Society for Human Resource Management reported that fifty-six percent of the employers who participated in their survey confirmed they were using social media in their hiring processes.[11] This represented a thirty-four percent increase from the survey conducted in 2008.[12] This steady increase in popularity has the potential to leave individuals vulnerable to an invasion of privacy and potential discrimination when securing employment, unless laws such as SNOPA and the PPA are enacted. However, employers are not alone, as schools have also followed suit, with admission decisions being somewhat influenced by individuals' social networking presence.

---

twitter-statistics/ (last visited May 15, 2013).

[8] LinkedIn, About Linked In, http://press.linkedin.com/about (last visited May 15, 2013).

[9] *Id*.

[10] Jeff Nolan, *OMG, LOL, AND WAY TMI—Social Media in the Hiring Process*, 15 No. 10 VT. EMP. L. LETTER 1, (2010); James J. Rooney & Diane M. Pietraszewski, *Crackdown on Employers' Access of Employees' Private Social Media Sites*, 19 No. 5 N.Y. EMP. L. LETTER 5 (2012) ("[i]n the past few years, social media has become an increasingly popular hiring tool for many employers . . . ."). A 2009 survey conducted on behalf of CareerBuilder.com received 2,667 responses from U.S. managers and HR professionals. Forty-five percent of the respondents said they used social media to screen candidates. An additional eleven percent reported that they planned to start using social media to screen applicants in the near future. Nolan, *supra*, at 1.

[11] *See Higher Productivity, Preparing Higher Skills: Preparing for a New Hiring Cycle*, WORKPLACE VISIONS, Society for Human Resource Management, Issue 2, at 1 (2011), http://www.shrm.org/Research/Future WorkplaceTrends/Documents/11-0277%20Workplace%20Visions %20Issue% 202-viewonlyFNL.pdf.

[12] *Id*.

III.PROBLEM

A. Potential for Fraud on the Internet

The unfortunate reality is that the Internet and social media networks do contain fraudulent information.[13] Therefore, the profile[14] or other information a school or employer finds on the candidate when snooping around the Internet is not necessarily accurate and it, nor may not, have even been posted by the individual candidate.[15]

To demonstrate this reality, consider the 2010 American documentary film, Catfish.[16] The documentary follows a man, Nev, who develops an online relationship with someone he believes to be named Megan, with whom he develops a romantic interest.[17] Throughout the course of this long-distance online relationship,

---

[13] *See* Ian Brynside, Note, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 446 (2008) ("[E]mployers should remember that an applicant's online persona does not always provide an accurate, reliable, or complete picture of the person."); Ebnet, *supra* note 2, at 307 (discussing some opposed to employers using social media to aid in hiring decisions cite "concerns over the trustworthiness and authenticity of information obtained from the Internet.").

[14] Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. OF COMPUTER-MEDIATED COMMC'N 1, (2007), *available at* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (Profiles are unique pages where an individual fills out information that typically includes data points like age, city of residence, interests, and an "about me" summary and a photo. Some sites offer advanced profile features such as multimedia content. The owner of the profile is often allowed to establish some security settings to restrict its visibility and accessibility for other users).

[15] *See* Ebnet, *supra* note 2, at 317 (discussing how third parties have the ability to post misleading information online without the user's agreement); Miller, *supra* note 2, at 544.

[16] Peter Debruge, *Review: 'Catfish'*, VARIETY, Jan. 23, 2010, http://www.variety.com/review/VE1117941945.html?categoryid=31&cs=1.

[17] *Catfish*, WIKIPEDIA, http://en.wikipedia.org/wiki/Catfish_(film) (last visited Jan. 15, 2013).

Nev receives artwork, pictures, and music from "Megan."[18] However, after investigations and an impromptu visit to "Megan", he learns everything is a lie.[19] First, "Megan", is really a woman named Angela, who is married with children.[20] Second, the social network pictures of "Megan" were later discovered to belong to a woman who lives in a different state.[21] The original songs received during their "relationship" were the work of other people on YouTube.[22] Even the artwork Nev received, which "Megan" claimed her daughter created, was in fact, created by Angela.[23]

Despite some who question the documentary's complete authenticity, the documentary has been recognized by many, including receiving attention from Time Magazine. Time Magazine's article suggests that after seeing the documentary, "you're likely to think this is the real face of social networking."[24]

As a result of the show's popularity, this documentary was developed into a reality television show, which focuses on the lives of real individuals involved in online relationships in search of discovering if their "significant other" is truly who they say they are.[25] This documentary demonstrates the real concern of an individuals' susceptibility to having another person steal their pictures, name, or other identifying information and as a result, to be misjudged based on information posted online. Moreover, it

---

[18] *Id.*; Mary Pols, *Fish Tale*, TIME MAGAZINE, Sept. 27, 2010, http://www.time.com/time/magazine/ article/0,9171,2019606,00.html.

[19] *Id*.

[20] *Id*.

[21] *Id*.

[22] *Id.*; *see also* Jim Hopkins, *Surprise there is a Third YouTube Co-Founder*, USA TODAY, Oct. 11, 2006, http://usatoday30.usatoday.com/tech/news/2006-10-11-youtube-karim_x.htm (YouTube is an online video sharing site that broadcasts 100 million short videos daily).

[23] Pols, *supra* note 18.

[24] Kara Warner, *'Catfish' MTV Show Brings Online Love Stories to Life*, MTV NEWS, http://mtv.com/news/articles/1689098/catfish-online-love-reality-show.jhtml.

[25] Pols, *supra* note 18; *Catfish*, ROTTEN TOMATOES, http://www.rottentomatoes.com/m/catfish/ (last visited Dec. 3, 2012) (the documentary held an 82% fresh rating).

shows how easily an individuals' privacy can be violated and how personal information may be misused. When an employer screens online profiles to judge potential hires, there is no way to know if the information they find is a fake profile generated by compromised data. For example, in a quarterly report filed by Facebook with the United States Security and Exchange Commission, it reported that Facebook suspects that 1.5 percent of their 995 million accounts may be fraudulent. [26] This figure equates to over 14 million accounts.[27]

B. The Inadequacies of Existing Laws

The enactment of SNOPA and the PPA is of critical importance. The existing framework of the law affords limited protection to one's security and privacy. Some initial court decisions also provide a glimpse into the court's apprehension to limit potential employer's actions and their snooping around the public's social media pages.[28] In *Maremont v. Susan Fredman Design Group, Ltd.*, the court denied a plaintiff's privacy claim based on the tort claim of intrusion upon exclusion.[29] In this case, the defendant used the plaintiff's social networking credentials without permission to access her Facebook and Twitter accounts.[30]

The court held that the information on those social networking sites were not private because the plaintiff had over 1,250 followers, and thus, subsequently dismissed the claim.[31] This decision was reached despite the fact that the Restatement of Torts

---

[26] Facebook, Inc., Quarterly Report (Form 10-Q) 47 (June 30, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1326801/000119312512325997/d371464d10q.htm#tx3714164_14.

[27] 995,000,000 multiply by 1.5% = 14,325,000.

[28] Maremont v. Susan Fredman Design Grp., Ltd., No. 10 C 7811, 2011 WL 6101949, at *7-8 (N.D. Ill. Dec. 7, 2011).

[29] *Id*.

[30] *Id*.; *see generally* James Bessen & Eric Maskin, *Intellectual Property on the Internet: What's Wrong with Conventional Wisdom?* (2004), http://www.researchoninnovation.org/iippap2.pdf.

[31] Maremont, 2011 WL 6101949, at *7-8.

indicates that the tort intrusion upon exclusion applies "when someone investigates or examines a person's private matters, including opening one's email."[32] Specifically, the tort of intrusion is "one who intentionally intrudes. . .upon the solitude of seclusion of another or his private affairs or concerns, subject to liability. . . if the intrusion would be highly offensive to a reasonable person."[33] This outcome is just one example of how existing laws, such as the Stored Communications Act (SCA), Computer Fraud and Abuse Act (CFAA), and the Fair Credit Reporting Act (FCRA) are inadequate by failing to provide the necessary protections given the advancements in technology, as outlined later in this article.[34] Consequently, applicants whom may be concerned about privacy rights are currently forced to rely on the inadequate privacy laws and the court's interpretation of the applicant's reasonable expectation of privacy.[35]

Modern decisions demonstrate that courts are not interpreting existing privacy laws to recognize individuals' reasonable expectations of privacy when he or she simply has a

---

[32] Alissa Del Riego et al., *Your Password or your Paycheck*, 16 No. 3 J. INTERNET L. 1, 19 (2012); Restatement (Second) of Torts § 652B, cmt.b (1977).

[33] Restatement (Second) of Torts § 652B (1977).

[34] Riego et al., *supra* note 32, at 18 ("In the United States, privacy law has largely been formulated around the physical realm to deal with individual's reasonable expectations of privacy in physical spaces, such as the home or provide desk drawers, lockers, bathrooms, etc. These spaces typically are easily defined, but with the risk of modern technology that travels between person and work spheres, protecting the privacy of digital spaces has become quite sticky for courts and legislatures.").

[35] *See id.* (Job applicants' privacy rights, whether under the Fourth Amendment, privacy torts, or other statutes are framed around an inquiry into the applicant's reasonable expectation of privacy); Feuer, *supra* note 2, at 475 (discussing in the absence of a precedent from the Supreme Court, lower courts have ruled that there is no reasonable expectation of privacy if the communication is made to a large audience, including posts on a social media website); Hector Gonzales et al., *Do Privacy Rights in Electronic Communications Exists?*, N.Y. L.J. (Jan. 17, 2012), http://www.dechert.com/files/Publication/f31dfdde-be79-4c66-9736-0c9f855e9c99/Presentation/PublicationAttachment/87a8a2bb-0ac1-4153-8356-1ebaa418f78f/GonzalezMcGuireKahan%20-%20NYLJ%20-%201-17-2012.pdf.

lengthy friend list or following.[36] It does not seem persuasive to courts that a user can opt to preclude all others from seeing posted information, as Court decisions conclude that when a friend count is too high, one may be vulnerable to snooping because the user has made their information too public.[37]

Since the role of the judiciary is merely to apply the enacted laws, it is legislature's responsibility to take actions necessary to clearly establish that an individual's rights will not be compromised simply due to technological advancements.[38] The judicial branch needs such a clear and transparent message so it can have the power to enforce the privacy protections due to the people. By failing to establish such a standard, the government demonstrates its acquiescence to the trend.[39] Absent the action of the legislature, we are really asking for the courts to act beyond its scope and to legislate since the legislature is not keeping up with the times.[40]

Until appropriate action is taken, the desire will continue to grow for employers and educational institutions to perpetuate snooping activities because it has proven useful in obtaining a seemingly more holistic picture of the candidates.[41] Whether these "profiles" are accurate or not, employers and schools are snooping in the belief that they are getting a clearer picture of a candidate. The theory of Media Richness, considers the medium of the

---

[36] *Maremont*, 2011 WL 6101949, at *7–8.

[37] *Id*. at *8 n.2.

[38] *See* Riego et al., *supra* note 32, at 23 ("US laws must be tailored and interpreted to clearly address this oncoming trend." Suggesting that "the law should also provide applicants and employee clearer remedies and preventative measures against such intrusions.").

[39] *See* Ebnet, *supra* note 2, at 308 (citing Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., Bureau of Consumer Prot., Fed. Trade Comm'n, to Renee Jackson, Esq., Nixon Peabody, LLP (May 9, 2011), *available at* www.ftc.gov/os/closings/110509social-intelligenceletter.pdf).

[40] *See, e.g.*, Feuer, *supra* note 2, at 475 (discussing SCA was enacted by Congress in 1986, there is a "pressing need for statutory reform" since the SCA has not "kept up with the drastic changes in technology.").

[41] *See* Riego et al., *supra* note 32, at 18 ("[r]ecent studies have shown that an individual's OSN [online social network] profile can provide an accurate window into the individual's personality and character.").

communication used and its true effectiveness.[42] Communication is found to be increasingly effective when it is more "rich," with the best medium of communication being face-to-face contact.[43] The mediums of communication found to be the least "rich," or the least effective, under this theory are those such as written communication.[44] By creating a greater separation between the contact of the employer or school with the candidate, the entities conducting the search reduce their likelihood of garnering a true and accurate understanding of the candidate. Snooping would be at the lowest level of effectiveness under this theory, even less rich than sending an email, as it does not involve any directly intended communication at all. Candidates for employment or candidates for admission into educational institutions do not intend posted items on their profile be aimed at hiring or admissions personnel, but rather use it as a social forum. Moreover, the candidates do not push themselves onto the admissions or hiring personnel, but rather the personnel initiate direct and purposeful action to acquire this information. As a result, stories will continue to emerge about the snooping into personal pictures, comments, and posts, unless something is done to restrict this behavior.[45]

Other failed avenues of protection that snooping victims have attempted to seek protection and justice includes the Stored Communications Act (SCA) and the Computer Fraud and Abuse Act (CFAA). For employment candidates, these laws are not

---

[42] *See generally* Richard L. Daft & Robert H. Lengel, *Information Richness: A New Approach to Managerial Behavior and Organizational Design* 5–9 (1983), http://www.dtic.mil/dtic/tr/fulltext/u2/a128980.pdf.

[43] Robert Lengel & Richard L. Daft, *The Selection of Communication Media as an Executive Skill*, 2 THE ACAD. OF MGMT. EXEC. 225 (1989).

[44] *Id*.

[45] *See* Shannon McFarland, *Job Seekers Getting Asked for Facebook Passwords*, USA TODAY, Mar. 21, 2012, http://usatoday30.usatoday.com/tech/news/story/2012-03-20/job-applicants-facebook/53665606/1; *Have You Ever Shard Your Facebook Password?*, Poll, ABA. J. (Apr. 3, 2012), http://www.abajournal.com/polls/P36/ (reporting that less than one percent of respondents have been requested by their employer to provide their Facebook password).

failsafe.[46] For example, the CFAA requires that a plaintiff demonstrate that they have suffered at least 5 thousand dollars in damages within a twelve month timeframe to be eligible to bring a claim.[47] Meanwhile, the SCA does not provide any coverage for electronic communication that can be easily accessed by the public.[48] The SCA has been criticized for this gap and has been described as failing "to provide a clear framework for understanding whether a user has a reasonable expectation of privacy in his communications stored in the cloud."[49]

Similarly, the framework under the Fair Credit Reporting Act (FCRA) also fails to close the gaping hole of regulations protecting privacy.[50] While the FCRA does impose requirements for consent and notice for background checks that may involve viewing social media content, it fails in that it is only applicable to background screenings conducted by a third-party.[51] This failure is due to the type of information available on social networking sites, which enables more organizations to successfully conduct their own independent search without engaging assistance of third party screening companies.[52]

---

[46] *See* Riego et al., *supra* note 32, at 21 (stating most job applicants would have difficulty demonstrating they suffered the economic loss or damages as a result of an invasion of privacy from "a snooping employer" as required under the CFAA); Feuer, *supra* note 2, at 475.

[47] 18 U.S.C. § 1030(g) (2008); 18 U.S.C. §1030 (c)(4)(A)(i)(I) (2008).

[48] *See* Steven C. Bennett, *Civil Discovery of Social Networking Information*, 39 SW. L. REV. 413, 422 (2010).

[49] Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 645 (2011); *see also* Mark S. Sidoti et al., *How Private is Facebook?*, N.Y. L.J., Oct. 4, 2010, at S14 (the SCA is "outdated and not ideally structured to address modern electronic communications disclosure and privacy issues.").

[50] Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681t (2006).

[51] *Id.*; *see* Ebnet, *supra* note 2, at 308 (discussing social network searches conducted by employers on their own do not impose liability established under the FCRA because it is not a background check being performed by a third party).

[52] *See* Brynside, *supra* note 13, at 459 (the amount of applicant information available online makes it "easily accessible" for employers).

More importantly, absent adequate laws, potential employees and students are subject to discrimination.[53] Whether intentional or not, a potential employer or educational institution will have information about the candidate after viewing social networking sites that they would not ordinarily have the legal right to obtain during an interview process; this would be prohibited under Title VII of the 1964 Civil Rights Act, which requires that employment decisions not be based on "race, color, religion, sex, or national origin."[54] Whether or not the employer used this information in their decision is extraneous; the fact that they had this information still introduces a plausible argument that the decision was a biased one.[55]

For example, in *Gaskell v. University of Kentucky*, the plaintiff was able to use evidence of an employer's Internet searches as support for a claim of discrimination that allegedly

---

[53] Riego et al., *supra* note 32, at 23 ("There exists a potential for significant abuse, misuse, and misinterpretation of information, especially at the hands of employers.").

[54] 42 U.S.C. § 2000c-2(a)(1) (2006); *See* Riego et al., *supra* note 32, at 21 (discussing a plausible argument for injuries to employment candidates could arise under discrimination law due to Title VII of the Civil Rights Act of 1964, which serves to prohibit employment decisions based on "race, color, religion, sex, or national origin" as well as the expansion of protections under various state enacted laws prohibiting employment decisions based on age, marital status, legal activities, political activities, sexual orientation, or disabilities).

[55] Heather R. Huhman, *Why You Could Be Breaking The Law By Researching Job Candidates Online*, BUSINESS INSIDER (Mar. 9, 2011), http://www.businessinsider.com/is-it-legal-to-research-a-job-candidate-online-2011-3 (Attorney Jason Shinn of E-Business Counsel, PLC discussing how knowledge obtained after internet search could, "create a link between a denial of employment and a violation of applicable employment or labor law" even if what was learned through the social media search was not the reason for employer's hiring decision); Diane Pfadenhauer, *Social Networking Sites and Employment: Watch out for GINA*, STRATEGIC HR LAWYER (June 15, 2010), http://www.strategichrlawyer.com/weblog/2010/06/social_networki.html (mentioning the problem of how an employer really demonstrate their decision was not based on information they found online).

occurred during the hiring process.[56] The university had an opening for a director's position.[57]

An agent of the university performed an online search of the applicant, C. Martin Gaskell, and the results included an article that discussed astronomy and the Bible.[58] The individual who found the article then sent an email stating, "the real reason we will not offer him [Gaskell] the job is because of his religious beliefs."[59] As a result, Gaskell was not offered the position.[60] He subsequently sued for religious discrimination, and the case was later settled.[61]

A recent study performed by a leading career and resume-building website, LiveCareer.com, demonstrates just how prevalent the practice of snooping is becoming.[62] The survey collected the views of over 6,600 users.[63] Results of the survey indicate that over forty-six percent of company executives believe "a company ***should*** review a candidates profile before extending a job offer."[64] Even more revealing was that forty-one percent believe that companies have the ***right*** to deny an offer of employment based on what they observe within the applicant's online profile.[65] These sentiments directly defy existing laws that prohibit asking about race, gender, religion, age, pregnancy, or sexual preference during the interview process; yet these characteristics are exactly the type of information that is readily available when viewing social networking profiles.[66]

---

[56] Gaskell v. Univ. of Kentucky, No. CIV.A. 09-244-KSF, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010).
[57] *Id*.
[58] *Id*.
[59] *Id*.
[60] *Id*. at *6.
[61] *Id*.
[62] Daniel Hong, *Your Facebook Profile Could Affect Your Hiring Potential*, PRWEB (May 31, 2012), http://www.prweb.com/pdfdownload/9556895.pdf.
[63] *Id*.
[64] *Id*. (emphasis added).
[65] *Id*. (emphasis added).
[66] *Id.* (James Freundlick, co-CEO of Live Career North America discusses that most people are aware of the restricted topics that must be avoided during the interview process but "[w]hat people may not realize is the degree to which

As a result, even if a decision maker has the best intentions in viewing these profiles, it cannot definitively be said that protected characteristics or classifications are not being weighed in the hiring or admissions process. For those who are not neutral, these practices will facilitate discrimination.

Therefore, the growing sense of "right" or "entitlement" to research candidates online is crossing the customary boundaries and is stretching into areas that will welcome discrimination if SNOPA and the PPA are not passed. This recent shift in modern day hiring and admissions procedures significantly deviates from the customary approach to evaluating potential candidates.[67] Consequently, there is ample room for a third party to incorrectly interpret the context of your messages, comments, and pictures. However, pressure is mounting to take action to afford people the protection they deserve. For example, the Maryland Department of Corrections reported that they suspended their social media password requirement policy for applicants for a period of forty-five days after receiving negative publicity for this procedure.[68] In another instance, the city of Bozeman, Montana attempted to justify their practice by stating they had a duty to be thorough in their

---

hiring manager can glean personal information about candidates by poking around their Facebook page.").

[67] Riego et al., *supra* note 32 at 17 (discussing as a society was are familiar with and accept the typical application ritual of submitting a resume that will reveal our job history, hobbies or interests, and a list of references); Ebnet, *supra* note 2, at 308 ("[h]istorically, employers relied on written applications, questionnaires, interviews, references, and background checks to screen job applicants."); *see generally* Rochelle B. Ecker, Comment, *To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee*, 63 UMKC L. REV. 251, 255-61 (1994) (discussing traditional methods of conducting pre-employment screening).

[68] Molly DiBianca, *Md. Agency Suspends Facebook-Password Policy*, DEL. EMP. L. BLOG (Feb. 28, 2011), http://www.delawareemploymentlawblog.com /2011/02/md-agency-suspends-facebookpas.html; David L. Hudson, Jr., *Site Unseen: Schools, Bosses Barred from Eyeing Students', Workers', Social Media*, ABA J. (Nov. 1, 2012, 2:10 AM),http://www.abajournal.com/mobile/ mag_article/site_unseen_schools_bosses_barred_from_eyeing_students_workers _social_media/?utm_source=maestro&utm_medium=email&utm_campaign=tech _monthly.

consideration of applicants.[69] Later, a spokeswoman for Bozeman, Montana announced that the city would no longer ask applicants for their social media credentials as part of their "background check" after receiving harsh criticism when news of their hiring practice became known.[70]

Unfortunately, this problematic trend also appears in schools and affects students of all ages.[71] In some instances, schools have required students to hand over their personal username and passwords, justifying this practice as a measure to curb bullying or other behavioral issues at school.[72] However, some colleges have gone even further and are not only demanding access to the social networking sites, but are also requiring students to install spy software on their computers.[73] Attorney Bradley Shear, who has written extensively on social media and legal implications, has called what is happening in colleges an "epidemic."[74] He questions these practices saying, "[w]hen did it become legal for public universities to be able to require their students to download spying software onto their personal iPhones or social media accounts to monitor pass-word-protected digital content?"[75]

From personal experience, law school administrations warns their students to be mindful of their online presence and to be prepared to hand over personal credentials to the Florida Bar if deemed necessary. In July 2009, the Florida Board of Bar

---

[69] *Id*.

[70] Molly DiBianca, *How to Become an Employer of Last Resort: Require Applicant's Facebook Passwords*, DEL. EMP. L. BLOG (June 28, 2009), http://www.delawareemploymentlawblog.com/2009/06/how-to-become-an-employer-of-1.html.

[71] Hudson, *supra* note 68.

[72] *Id*.

[73] *Id*.

[74] *Id*. Attorney Bradley Shear is an adjunct professor at The George Washington University and is a well-known attorney and author. His private practice focuses on Social Media and Internet law among other things. Mr. Shear was also the first private practice lawyer within the United States to work with the state government to assist with drafting social media law. A list of credentials and published works is available at http://shearlaw.com/attorney_profile.

[75] *Id*.

Examiners adopted a policy that will include viewing applicants' social media pages in specific situations.[76] To date, this request has not been made of me, but it seems that there is no limit to the span of this intrusive scourge. The ironic polarization of this issue is that it seems there is a large segment of this population that may be vulnerable to this intrusive behavior, which is being promulgated by various industries—including legal and government entities—and at all levels from young children to corporate America. Despite the growing concerns as evidenced by individual states' actions, these intrusions continue to occur.

While the focus of this article is on employment applicants and students, even after being hired individuals do not escape the prospect of employers snooping around their online profiles."[77] Protection of privacy interests hinges on whether legislation is enacted to ensure the proper protections are secured for people, while still striking a balance with the organizations' legitimate needs to screen applicants or students. Otherwise, we all may be subjected to these intrusive practices and policies, regardless of age, regardless of industry, and regardless of whether you are in school, seeking employment, or even trying to maintain a job.

Despite the absence of an all-encompassing law or laws that have been modified to keep stride with technological advancements, there is hope. States have stepped up to the plate and enacted laws that mitigate the impositions created by these trends.

---

[76] Jan Pudlow, *On Facebook? FBBE May Be Planning A Visit,* THE FLA. B. NEWS (Sept. 1, 2009), https://www.floridabar.org/DIVCOM/JN/JNnews01.nsf/8c9f13012b96736985256aa900624829/d288355844fc8c728525761900652232?OpenDocument; *see also* Character and Fitness Commission, Final Report to Supreme Court of Florida, 8–11 (Mar. 2, 2009),http://www.floridasupremecourt.org/pub_info/documents/2009_FBBE_Character_Fitness_Report_Short_Version.pdf.

[77] *See generally* Rooney, *supra* note 10; Riego et al, *supra* note 32; Feuer, *supra* note 2.

C. Current Protection for Students:

The Higher Education Privacy Act (HEPA), which was passed in Delaware in July 2012, is one example of the much needed protection for college students to guard against being compelled to release their private social media credentials to the school leadership. HEPA prohibits any academic institution from requesting social media credentials or any other electronic identifiers from a student or applicant.[78] HEPA was written not only to encompass social media accounts, but also any electronic account, including e-mail.[79] It also precludes academic institutions from asking for a student or applicant to log onto their social media profiles in the presence of its agent, deploying any type of electronic tracking mechanism, accessing a student's or applicant's online profile or account in directly, or making a request or mandate for a student or applicant such as "friending"[80] their accounts.[81]

Delaware State Representative, Darryl Scott, said, "I introduced the legislation to protect our students' First and Fourth Amendment rights. If a student is required to disclose their postings, as part of the college application process, would they write and share their thoughts freely? My concern was that they would not."[82] Attorney Bradley Shear points out that the law is really protecting both parties involved—the school and the student.[83] It also seems that HEPA attempts to strike a reasonable balance to protect the students, while equipping the institutions with a means to take action when certain exceptions arise, such as

---

[78] Del. Code Ann. tit. 14, § 8103 (West 2012).
[79] *Id*.
[80] CAROLYN ABRAM & LEAH PEARLMAN, FACEBOOK FOR DUMMIES 91 (4th ed. 2012) "Friending" is the act of adding or granting access to another individual's social media profile so they have access to your social media profile. As a "friend" another user will have access to see information, pictures, messages and other media that you have given the social media site permission to share with those who have the privilege of "friend." *Id*.
[81] *Id*.
[82] Hudson, *supra* note 68.
[83] *Id*.

scenarios involving health and safety.[84] Another reason laws like HEPA are important is because they ensure that school officials cannot escape liability for alleged violations of the students' constitutional rights by raising the defense of qualified immunity on the basis of the law not being clearly established.[85] Unfortunately, the HEPA does not provide protection for students who are in kindergarten through high school.[86] However, the state has indicated that it expects there will be negotiations over including such a provision to cover these students during the next legislative session.[87]

Like Delaware, California has also approved legislation to stop schools from demanding the students' social media credentials.[88] California Senator Leland Yee stated, "California is set to end this unacceptable invasion of personal privacy. The practice of employers or colleges demanding social media passwords is entirely unnecessary and completely unrelated to someone's performance or abilities."[89]

D. Current Protection for Employees

As employees are no different from students in that their privacy is precious, some states are beginning to take action to stop snooping employers. In 2012, both Maryland and Illinois passed

---

[84] *Id*. The Act allows for the public safety officials to monitor social media activity if there are "reasonable, articulable suspicions of criminal activity." They also have the authority to conduct an "investigation, inquiry, or determination conducted pursuant to an academic institution's threat assessment policy or protocol." *Id*.

[85] *Id.* Attorney, Wallace Hilke, discusses the law saying, "Legislation prohibiting school officials from forcing students to disclose passwords is a good idea because it would completely eliminate the qualified immunity defense, as there would be a clearly established statutory authority." *Id*.

[86] *Id*. State Representative Darryl Scott removed a provision that would have also extended cover to K-12 because there was not sufficient agreement for it to remain amid concerns that it would afford protection to bullies. *Id*.

[87] *Id*.

[88] Hudson, *supra* note 68.

[89] *Id*.

legislation that would ban employers from seeking access to their employees' electronic sites under the User Name and Password Privacy Protection and Exclusion Act and the Illinois Right to Privacy in the Workplace Act, respectively.[90] With the growing concern over this issue, Senators have begun asking the Department of Justice and the Equal Opportunity Commission to investigate the matter and make a determination of whether federal law is being violated. As of May 2012 there has been no response.[91]

Moreover, notice where this leaves applicants—with virtually no protection, because the existing laws, like those previously mentioned, afford at best meager protections. Now, we turn our attention to SNOPA and the PPA to better understand what these proposed laws can do for us all and the effective potential they have on closing the door for snooping schools and employers.

IV. ARGUMENT

A. The Solution—Enactment of SNOPA and the PPA and Why it is so Important

Currently, there are extensive loopholes in the existing laws making existing laws inadequate to provide protection for the privacy of society. Therefore, it is necessary to enact federal laws to ensure the citizens of this country are afforded the protections set forth in the United States Constitution.[92] While trends are showing

---

[90] S.B. 433, 430th Md. Gen. Assembly (2012); H.R. 4432, 97th Ill. Gen. Assembly (2011).

[91] *See*, Hudson, *supra* note 68 (citing that Senators Charles Schumer of New York and Richard Blumenthal of Connecticut have called for an investigation by the Department of Justice and the Equal Opportunity Commission to determine if federal laws are being violated by those who are requiring individuals to provide their social media credentials).

[92] U.S. CONST. amend. IV ("[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."); Hudson, *supra* note 68 (describing attorney Bradley Shear's discussion on the fact that there is neither a federal law or a Supreme Court decision that speaks to this issue, therefore, "[N]ew laws are needed to clarify the legal landscape.").

that states have started to put laws in place to protect their residents, failure to act on the part of the federal government would create the potential for a disparity between those residents of states who are covered and the citizens of the United States who reside in locations that have not taken steps to grant the protection.

This matter is getting more attention, which may force legislative changes. New legislation has the potential to change the snooping trend by creating a new mandate preventing employers and schools from continuing with their snooping practices.[93]

In April 2012, State Representative Elito Engel introduced the Social Networking Online Protection Act (SNOPA), which is also known as House Resolution 5050.[94] SNOPA is critical to the privacy of all individuals, because it would establish clear law that specifically addresses what behavior would be prohibited for employers and schools. Particularly, SNOPA would make it unlawful for an employer to require an employee or applicant for employment to provide a username, password, or any credential information that would enable the employer to gain access to electronic media tied to the applicant, including e-mail accounts and personal accounts on social networking sites. In addition, it would be unlawful to discriminate against, deny employment, or threaten action against any applicant who declined to provide their online credentials.[95] The bill is thorough in that it includes an anti-retaliation provision prohibiting adverse employer action taken against an applicant for filing a complaint or participating in activities related to reporting a violation occurring under SNOPA.[96] It is also important to note that SNOPA defines an "employer" as "any person acting directly or indirectly in the interest of an

---

[93] Hudson, *supra* note 68. Attorney Bradley Shear supports this proposition stating, "I believe such legislation will eventually become the norm, because public policy and case law has indicated that requiring accessed to password-protected digital content may be against the law." *Id*.

[94] H.R. 5050, 112th Cong., 2d Sess. (2011).

[95] *Id*.

[96] *Id.*

employer in relation to an employee or an applicant for employment."[97]

In addition, SNOPA specifically provides for the same protection to existing employees. If an employer violates the proposed law, it would result in a civil penalty of up to 10 thousand dollars. It authorizes the secretary of labor to seek injunctive relief to restrain violations and require compliance.[98] Moreover, SNOPA law will grant the federal courts jurisdiction to issue appropriate relief.[99]

Similarly, SNOPA would also protect some of the children and students of educational organizations who have been left out by some of the relatively new state laws.[100] Moreover, SNOPAwould prevent some educational institutions and education agencies from asking students and applicants for online credentials to gain access to the same type of online content that the employment organizations have been prohibited from seeking access.[101]

After the introduction of SNOPA, the Password Protection Act of 2013 (PPA),S.1426 and H.R. 2077, was introduced in the House and Senate.[102] Like SNOPA, the proposed legislation would prohibit employers from demanding a person to provide others with access to their social networking accounts.[103] The PPA would serve to amend current law and prohibit an employer from obtaining credentials to retrieve information on a protected computer so long as it is not the employer's protected computer.[104] This law would also provide protection against retaliatory actions against applicants

---

[97] *Id*.; *see also* Tamara R. Jones, *Snopa Proposed to Prohibit Snooping*, 23 NO. 9 TEX. EMP. L. LETTER 3 (2012).

[98] *See* Jones*, supra* note 97.

[99] *Id*.

[100] H.R 5050, 112th Cong., 2d Sess. (2011).

[101] Rooney & Pietraszewski, *supra* note 10. Higher learning and local educational agencies receiving funds under Title IX of the Elementary and Secondary Education Act of 1965 are precluded from seeking access to the applicant's online accounts or social networking sites. Note: the bill has separate provisions addressing those entities. *Id.*

[102] Hayes & Cooley, *supra* note 1.

[103] *Id*.

[104] *Id*.

and employees by prohibiting employers from discriminating or discharging for failing to give authorization to access to a potential employee's computer or for filing a complaint.[105] Together, the PPA and SNOPA provide full coverage to put an end to snooping. There are similarities in the protection afforded under these proposed laws, which serves to close all potential loopholes. Simply, individuals do not have to release their credentials, nor do they have to be fearful of retaliation, for they have protection available under SNOPA and the PPA.

B. What If SNOPA and/or the PPA Fails?

If the legislature does not agree to enact SNOPA and/or PPA, we will be forced to rely on each state to enact laws that will protect its residents' privacy rights. Thankfully, several states have recognized the significant harm their residents' privacy absent new laws to address the ever changing technology landscape. While it should provide comfort that states have the autonomy to enact such legislation, it is still disconcerting that there could be a segment of the population who would remain vulnerable should their state choose not to act. The Constitution affords all citizens of this country protection and it has been interpreted to preserve a right to privacy.[106] As this note demonstrates, the intent of this precious amendment is being eroded with each day that passes. The passage of SNOPA and PPA is the most uniform way to ensure that all people are afforded equal protection and to ensure varying language between states does not preclude individuals from employment or educational advancements simply because of a snooping eye.

---

[105] H.R. 5684, 112th Cong., 2d Sess. (2011).

[106] *Olmstead v. US, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (*arguing the Framers had created a framework for "the right to be left alone."); U.S. CONST. amend. IX (establishing that even if a right is not specifically written in the Constitution it does not automatically mean that it does not exist).

V. CONCLUSION

Regardless of whether you are the student or employee who is vulnerable to being asked for your social media credentials or if you are an individual who is demanding these details, you should be aware of what SNOPA and PPA are and the purposes they serve. Just as individuals whose right to privacy is being established if SNOPA and PPA are signed into law, school organizations and employers should also be aware of the benefits it brings.

First, it clearly establishes the lines you can and cannot cross. Second, it may prevent exposure to unintended litigation through clearly establishing rules. SNOPA and the PPA aids by ensuring your organization does not engage in activity that can give the appearance that hiring or admission decisions were, in part, based on protected criteria, such as race, age, religion, or sexual orientation. Such litigation would prove to be quite burdensome for organizations to manage and most importantly, would affect their bottom line.

The legal system should also welcome the enactment of these laws, so that it is the Legislature that is appropriately creating law, thereby giving the judicial branch a clear standard to follow. Furthermore, this law will mitigate the risk of relying on an otherwise ambiguous law, which creates splits among circuits and clogs the docket. To date, the case law has demonstrated the challenges that various state courts have faced with attempting to interpret outdated language of the diverse technology related laws and the great difficulty in determining how the recent developments in technology will impact the rights of each party to the litigation. Above all else, whether by day we sit on the side of the table that is demanding the social media credentials or not, we are all just people. Therefore, as a citizen of this county, you stand to be affected by a request to receive your credentials so someone else can snoop around your page.

Therefore, in addition to the legal basis for which these laws are of the utmost importance, there is also a moral and ethical consideration to be made here. Whether we apply the Golden Rule of treating others as we would like to be treated, the Utilitarian

theory of acting in a manner that creates the most happiness for all, or the Kantian principle where humans are never treated simply as a means to an end, but always also as ends in and of themselves, it certainly seems from both a legal and ethical perspective, protecting personal privacy is the way to go. Guarding one's privacy stands for treating someone else as we would expect to be treated (Golden Principle), it will promote the greatest happiness for all (Utilitarian Theory), and ensure we do not use each other as just a means or mechanism for the ends we seek. Rather, we both are in the position to consent to transact with each other in a harmonious manner as taught under the Kantian principle (student as an applicant to a school and applicant to a potential employer). SNOPA and the PPA promote all these theories and can ensure we are all protected.

If appropriate legislation is not enacted, it will be important for individuals to remain cognizant of the laws, or lack thereof, and what it really means for personal privacy. If states have not taken action to close the loopholes in the existing laws, this article advocates that individuals should consider taking action to petition local representatives to prompt their action to speak up and help promote the passage of the laws necessary to ensure the right to privacy is not squandered away any further. Given the times we are living in, with a compromised economy and job market, the last thing the people of this country need are roadblocks that inhibit their ability to get into the market place to provide for their families or to face vulnerability to discrimination or other hardships as a result of a wandering eye who scourers the social network for anything they can find. For these reasons, I leave you with a few questions. If your name were to be searched, would accurate information appear? Would a third party correctly interpret the context of your messages, comments, or pictures? Can an individual's personal ideologies be trusted to not have a negative impact on individuals' jobs, job offers, acceptances, or admittances? Are you comfortable with not having clearly established law that affords you redress should a violation occur? Given the appropriate scenario, are you satisfied with opportunities for certain individuals to have the ability to escape liability through defenses, such as qualified immunity, on the basis of law not being

clearly established at the time of an alleged constitutional violation? I hope the answers to all of these aforementioned questions, will be a definitive, “no.” For the answer to remedy all of these issues lies before us in the form of proposed legislation, SNOPA and the PPA.