SNOPA AND THE PPA_ DO YOU KNOW WHAT IT MEANS FOR YOU

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 not pass, the snooping could cause you trouble

By Angela Goodrum*

I. Introduction

II. Background
   Social Media and Its Popularity

III. Problem
   Potential for Fraud on the Internet
   The Inadequacies of Existing Laws
   Current Protection for Students
   Current Protection for Employees and Applicants

IV. Argument
   The Solution—Enactment of SNOPA and the PPA and Why it is so Important
   What if SNOPA and/or the PPA Fails?

V. Conclusion

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 equal opportunities for others, such as hiring personnel or admission offices, to snoop around, discriminate, and base their hiring and admission decision, in part, based on an individual’s online persona. 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.

This article defines social media and discusses its popularity. Next, this article covers
fraud on the Internet, and why it is a legitimate concern for applicants as there is no guarantee that the searches the potential employer or educational institution conducts will return legitimate data.

Section four will explain the importance of the passage of SNOPA and the PPA by revealing some of the inadequacies of existing privacy laws and demonstrating how these laws leave the United States population vulnerable. Sections five and six highlight some of the current protection afforded students, applicants, and employees and articulates why these laws insufficient.

Throughout this article there is discussion regarding issues that individuals have encountered with employers and schools as a result of these entities’ practices of snooping around using social media. Section seven of this article advocates the passage of both—SNOPA and PPA—and discusses alternative protection that may be afforded under other laws. In conclusion, this article will advocate for individuals to take action to prompt their local government to do what is necessary to ensure privacy rights are not squandered away. Further, argument will be made regarding the matters that individuals should consider if the laws do not fully provide coverage.

II. Background

Social Media and Its Popularity

Social media has been defined by the National Labor Relations Board as “various online technology tools that enable people to communicate easily via the internet to share information and resources….” Such social media sites would include Facebook, Twitter,

---

*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.

LinkedIn and other similarly situated sites. Social media has become a part of many individuals’ everyday lives, to the point where many do not go a day without interacting with some form of social media. Facebook is currently the leading social networking site and has garnered over one billion active users throughout the world. To put it in perspective, it has been said that if Facebook were a country, it would be the third largest in the world, larger than the United States but coming in after China and India. Even when on the move, people have social media by their side, with more than six hundred and four million active users accessing this leading social media site via their mobile devices.5

Also steadily increasing in popularity is Twitter, who has reported receiving 1 billion “tweets” per week with five hundred million users as of 2012. As of February 2011, Twitter was averaging four hundred and sixty thousand new account each day. Another popular social media site is LinkedIn, which operates the world’s largest professional network on the Internet—with more than seventy four million members in the U.S. as of January 9, 2013.

The fastest growing demographic on LinkedIn is reported to be students and recent college graduates, making up twenty million of LinkedIn’s members as of May 2012.

---

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, Note, 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 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 everyday millions of people use Facebook to keep up with their friends).


5 Facebook, http://newsroom.fb.com/Key-Facts


7 http://blog.kissmetrics/com/twitter-statistics/.

8 LinkedIn, http://press.linkedin.com/about

9 Id.
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.\textsuperscript{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.\textsuperscript{11} This result was a thirty-four percent increase from a survey conducted in 2008.\textsuperscript{12} This steady increase in popularity has the potential to leave individuals vulnerable to an invasion of privacy and potential discrimination when securing employment, or even seeking admission to educational institutions if the laws unless laws such as SNOPA and the PPA are enacted. Employers are not alone; schools have also followed suit and admission decisions are being determined, in part, by individuals’ social networking presence.

\textbf{III. Problem}

\textbf{Potential for Fraud on the Internet}

The unfortunate reality is that the Internet and social media networks do contain fraudulent information.\textsuperscript{13} Therefore, the profile or other information a school or employer finds when snooping around, is not necessarily accurate or even information the individual candidate has posted online.\textsuperscript{14} To demonstrate this reality, consider a 2010 American documentary film,

\textsuperscript{10} Jeff Nolan, \textit{OMG, LOL, AND WAY TMI—Social Media in the Hiring Process}, Vt. Emp’t Law Letter, 2010 (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); James J. Rooney, Diane M. Piiaszewski, \textit{Crackdown on Employers’ Access of Employees’ Private Social Media Sites}, 19 No. 5 N.Y. Emp. L. Letter 5 (May 2012) (“[i]n the past few years, social media has become an increasingly popular hiring tool for many employers…”).


\textsuperscript{12} \textit{Id}.

\textsuperscript{13} See Ian Brynside, Note, \textit{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, \textit{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.”).

\textsuperscript{14} See Ebnet, \textit{supra} note 2, at 317 (discussing third parties have the ability to post misleading information online without the user’s agreement); Miller, \textit{supra} note 2, at 544.
Catfish. The documentary follows a man, Nev, who develops an online relationship with someone he believes to be named Megan. Throughout the course of this long-distance online relationship, Nev receives artwork, pictures, and music from his “girlfriend.” However, after doing some investigating and making an impromptu visit to Megan, he learns everything is a lie. First, his girlfriend, Megan, is really Angela. Angela is a married woman with children. The social network pictures portrayed to be “Megan” were later found to have been taken from a woman who lived in a different state. The original songs received during their “relationship” were discovered to be taken from other people on YouTube. Even the artwork Nev received, which “Megan” claimed to have been created by her daughter, was in fact, created by Angela.

Despite some who question the documentary’s complete authenticity, the documentary has been recognized by many, including receiving attention from Time Magazine, whose article suggested that after seeing the documentary, “you’re likely to think this is the real face of social networking.”

As a result of its popularity among viewers, this documentary has now been turned into a reality television show, which focuses on the lives of real individuals who have been involved

---

18 Id.
19 Id.
20 Id.
21 Id.
22 Id.; Jim Hopkins, Jim, Surprise there is a Third YouTube Co-Founder, USA TODAY, available at 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 Id.
in an online relationship and who are in search of finding out if their “significant other” is who they say they are.\textsuperscript{25} This documentary demonstrates the real concern of an individuals’ susceptibility to having another person stealing their pictures, name, or other identifying information and as a result, may be misjudged based on information posted by another. When that 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 nine hundred ninety five million accounts may be fraudulent.\textsuperscript{26} This figure equates to over fourteen million accounts.\textsuperscript{27}

\textbf{The Inadequacies of Existing Laws}

The enactment of SNOPA and the PPA is of critical importance when one realizes the limited protection individuals may be afforded after analyzing the framework of existing laws. Moreover, 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.\textsuperscript{28} In \textit{Maremont v. Susan Fredman Design Group, Ltd.}, the court denied a plaintiff’s privacy claim that was filed based on the tort claim of intrusion upon exclusion.\textsuperscript{29} The defendant used the plaintiff’s social networking credentials without permission for the purpose of accessing her Facebook and Twitter accounts.\textsuperscript{30}

\textsuperscript{25} Pols, supra note 17; \textit{Catfish}, Rotten Tomatoes, http://www.rottentomatoes.com/m/catfish/ (the documentary held an 82\% fresh rating).
\textsuperscript{27} 995,000,000 divided by 1.5\% = 14,325,000
\textsuperscript{28} \textit{Maremont v. Susan Fredman Design Group, Ltd.}, No. 10-C-7811, 2011 WL 6101949 (N.D. Ill. 2011).
\textsuperscript{29} Id.
\textsuperscript{30} Id.
The court held that the information on those social networking sites could not be considered private because the plaintiff had over one thousand two hundred and fifty followers, and so the court dismissed the claim.\textsuperscript{31} This decision was reached despite the fact the Restatement of Torts indicates that the tort intrusion upon exclusion applies “when someone investigates or examines a person’s private concerns, including opening one’s email.”\textsuperscript{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.”\textsuperscript{33} This outcome is just one example of how existing laws are not adequate to provide the needed protection given the advancements in technology.\textsuperscript{34} Consequently, job 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.\textsuperscript{35}

As modern court decisions demonstrate, existing privacy laws are being interpreted to not recognize an individual as having the reasonable expectation of privacy just because he or she may have a lengthy friend list or following.\textsuperscript{36} It does not seem to be persuasive to courts that a user can opt to preclude all others from seeing their “posts,” pictures, comments or other

\textsuperscript{31} Id. at *7-8.
\textsuperscript{32} Alissa Del Riego et al, Your Password or your Paycheck, 16 No. 3 J. Internet L. 1, 18; Restatement (Second) of Torts § 652(B), cmt. b (1977).
\textsuperscript{33} Restatement (Second) of Torts § 652(B) (1977).
\textsuperscript{34} Riego et al, supra note 30, 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”).
\textsuperscript{35} See Riego et al., supra note 30, at 18 (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?: Courts Are Proceeding Cautiously, N.Y. L.J., Jan. 17, 2012, at S6.
information. Court decisions show if the friend count is too high, one may be vulnerable to the snooping.\textsuperscript{37}

Since the role of the judiciary is to apply the law that has been enacted, it is critical that the legislature take the action necessary to clearly establish that the protection of individual’s rights will not be compromised simply due to technological advancements.\textsuperscript{38} This clarity and clear message is what the judicial branch needs so it can be comfortable in enforcing the protections due to the people. By the government’s failure establish this clarity, it demonstrates that it has acquiesced to the trend.\textsuperscript{39} Otherwise, absent the action of the legislature, we are really asking for the courts to step in and legislate since the legislature is not keeping up with the times.\textsuperscript{40}

Until appropriate action is taken, the desire will continue to grow for the employers and educational institutions to perpetuate this activity because it has proven to be useful in obtaining a more accurate picture of the candidates.\textsuperscript{41} As a result, stories will continue to emerge about the intentional snooping into personal pictures, comments, and posts unless something is done to restrict this behavior.\textsuperscript{42}

To date, other snooping victims have attempted to seek protection and justice based on

\textsuperscript{37} \textit{Id.} at *8, fn. 2.
\textsuperscript{38} \textit{See} Riego et al., \textit{supra} note 30 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.”).
\textsuperscript{40} \textit{See}, e.g., Feuer, \textit{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”).
\textsuperscript{41} \textit{See} Riego et al., \textit{supra} note 30 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.”)
the Stored Communications Act (SCA) and the Computer Fraud and Abuse Act (CFAA).

However, for employment candidates, these laws are not failsafe.43 For example, the CFAA requires that a plaintiff demonstrate that they have suffered at least five thousand dollars in damages within a twelve month timeframe to be eligible to bring a claim.44 In addition, the SCA does not provide coverage for electronic communication that can be easily accessed by the public.45 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.”46

Furthermore, the framework under the Fair Credit Reporting Act (FCRA) also fails to close the gaping hole of regulations protecting privacy.47 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.48 However, due to the type of information available on these social networking sites, it enables more and more organizations to successfully conduct their own independent search without engaging assistance of third party screening companies.49

More importantly, absent adequate laws, potential employees and students are subject

43 See Riego et al., supra note 30 at 21 (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.
45 See Steven C. Bennett, Civil Discovery of Social Networking Information, 39 Sw. L. Rev. 413, 422 (2010).
46 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”).
48 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).
49 See Byrnside, supra note 3, at 459 (the amount of applicant information available online makes it “easily accessible” for employers).
to discrimination. Whether intentional or not, a potential employer 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, as prohibited under Title VII of the 1964 Civil Rights Act, which requires that employment decisions are not be based on “race, color, religion, sex, or national origin.”

Whether or not the employer used this information in their decision, the fact that they had this information still introduces a plausible argument that the decision was a biased one.

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 occurred during the hiring process. The university had an opening for a director’s position. 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. 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…” As a result, Gaskell was not offered the position. He subsequently sued for religious discrimination and the case was later settled.

---

50 Riego et al., supra note 30, at 23 (“There exists a potential for significant abuse, misuse, and misinterpretation of information, especially at the hands of employers”).
51 42 U.S.C. § 2000c-2(a)(1) (2006); See Riego et al., supra note 30, 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.).
52 Heather R. Huhman, Why You Could Be Breaking The Law By Researching Job Candidates Online, BUSINESS INSIDER, Mar. 9 2011, available at http://www.businessinsider.com/is-it-legal-to-research-a-job-candidate-online-2011-3 (Attorney Jason Shinn of E-Business Counsel, PLC discusses 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 (Jun. 15, 2010), available at http:// www.strategichrlawyer.com/weblog/2010/06/social_networki.html (mentions the problem of how an employer really demonstrate their decision was not based on information they found online).
54 Id.
55 Id.
56 Id.
A recent study performed by a leading career and resume-building website, LiveCareer.com, demonstrates just how prevalent this practice is becoming.\(^{57}\) The survey collected the views of over six thousand-six hundred users. Results of the survey indicate over forty-six percent of company executives believe “a company should review a candidates profile before extending a job offer.”\(^{58}\) 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 based on the applicant’s online profile.\(^{59}\) These sentiments are despite 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 social networking profiles are viewed.\(^{60}\) As a result, even if a decision maker has the best intentions, by viewing these profiles it cannot be said definitively that protected characteristics or classifications are not being weighed when the hiring or admission decisions are being made. Moreover, for those who are not neutral, these practices will facilitate discrimination.

Therefore, the growing sense of “right” or “entitlement” to research candidates is crossing the customary boundaries and is stretching into a large number of areas that will welcome discrimination if SNOPA and the PPA does not put a stop to it. This recent shift in modern day hiring procedures are a significant deviation from the customary approach to evaluating potential employment candidates.\(^{61}\)


\(^{58}\) Id. (emphasis added).

\(^{59}\) Id.

\(^{60}\) Hong, supra note 55 (James Freundlick, co-CEO of LiveCareer 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 hiring manager can glean personal information about candidates by poking around their Facebook page”).

\(^{61}\) Riego et al., supra note 30 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); Ebnets, 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)
However, pressure is mounting to do something 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.\textsuperscript{62} In another instance, a spokeswoman for Bozeman, MT announced that they 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.\textsuperscript{63} Initially, the company attempted to justify their practice by stating they had a duty to be thorough in their consideration of applicants.\textsuperscript{64}

Unfortunately, this problematic trend also appears in schools and is affecting students of all ages, from kindergarten through twelfth grade and even well into college.\textsuperscript{65} In some instances, schools have required students to hand over their personal username and passwords and are justifying this practice as a measure used to curbing bullying or other behavioral issues at school.\textsuperscript{66} However, some colleges has even gone a step further and are not only demanding access to the social networking sites, but have also required students to install spy software on their computers.\textsuperscript{67} Attorney, Bradley Shear, who has written extensively on these topics, has called what is happening in colleges an “epidemic.”\textsuperscript{68} He calls these practices into question

\textsuperscript{63} Molly DiBianca, How to Become an Employer of Last Resort: Require Applicant’s Facebook Passwords, DELAWARE EMPLOYMENT LAW BLOG (June 28, 2009), http://www.delawareemploymentlawblog.com/2009/06/how-to-become-an-employer-of-l.html
\textsuperscript{64} Id.
\textsuperscript{65} Hudson, supra note 60.
\textsuperscript{66} Id.
\textsuperscript{67} Id.
\textsuperscript{68} Id.
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 account to monitor password-protected digital content?” 69

Even speaking from personal experience, I know I have been told that as a law school student, I should be prepared to hand over my personal credentials to the Florida Bar if deemed necessary. 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 there is a large segment of this population that may be vulnerable to this intrusive behavior, which is being promulgated by many different industries—including legal and government entities—and at all levels from young children to corporate America. Most seem to be against it, and yet it continues.

In addition, while the focus of this article is on pre-employment and students, individuals are not safe even after they’ve heard those sweet words, “you’re hired.” 70 Hopefully, at this point, it is becoming ever so clear that we all may be subjected to these intrusive practices and policies, regardless of your age, regardless of your industry, and regardless of whether you are in school, seeking employment, or even trying to maintain your job. An individual’s protection hinges on whether legislation is enacted to ensure the proper protections are secured for the people, while still striking the balance with the organizations’ legitimate needs to screen applicants and students.

Thankfully, in the absence of all-encompassing law or law that has been modified to be in keeping with the times, states have begun to step up to the plate and enact laws to mitigate

69 Id.
70 See generally Rooney, Diane M. Pietraszewski, supra note 10; Riego et al, supra note 30; Feuer, supra note 2.
the impositions created by these trends.

**Current Protection for Students:**

The Higher Education Privacy Act, which was passed 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. The Act prohibits an academic institution, both public and non-public, from requesting social media credentials or any other electronic identifiers from a student or applicant.\(^{71}\) The Act was also written to not only encompass social media accounts but any electronic account, including e-mail accounts.\(^{72}\) The institutions are also precluded from asking for a student or applicant to log onto their social media profiles in the presence of an agent of the school, deploy any type of electronic tracking mechanism, indirectly access the student or applicant’s online profiles or account via another person, or to make a request or mandate for the student or applicant associate such as “friending” their profile or accounts with the institution or its representatives.\(^{73}\)

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.”\(^{74}\) Attorney, Bradley Shear, points out that the law is really protection for both parties involved—the school and the student.\(^{75}\) It also seems this Act attempted to strike a reasonable balance to protect the students, yet equipping the institutions with a means to take action when certain exceptions arise, such as scenarios involving health and

\(^{71}\) Del. Code Ann. tit. 14, § 8103 (West).
\(^{72}\) Id.
\(^{73}\) Id.
\(^{74}\) Hudson, supra note 60.
\(^{75}\) Id.
Another reason laws like the Higher Education Privacy Act are important is because it also ensures 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. Unfortunately, the Higher Education Privacy Act does not provide protection for students who are in kindergarten through high school are not afforded protection under this Act. However, the state has indicated that it expects there will be negotiations over including a provision to cover these students during the next legislative session.

Like Delaware, California has also approved legislation to stop schools from demanding the students’ social media credentials. 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.”

**Current Protection for Employees**

Employees are no different from students in that their privacy is precious and some states are beginning to take action to stop the snooping employers. In 2012, both Maryland and Illinois have passed legislation that would ban employers from seeking access to their employees’ electronic sites, User Name and Password Privacy Protection and Exclusion Act and the Illinois Right to Privacy in the Workplace Act, respectively. With the growing concern

---

76 Id. (The Act allows for the public safety officials to monitor social media activity if there is a “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”).

77 Hudson, supra note 60 (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”).

78 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).

79 Id.

80 Id.

81 Id.

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.\(^{83}\)

Moreover, notice where this leaves applicants—with virtually no protection other than the meager protections afforded by the existing laws previously mentioned. So, let us turn our attention to SNOPA and the PPA to better understand what these proposed laws can do for us all and just how effective they have the potential to be in closing the door on these snooping schools and employers.

IV. Argument

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

Currently, there are large, gaping loopholes in the existing laws. Consequently, the existing laws are not adequate to provide protection for the privacy of society as has been shown throughout the discussion of this note. Therefore, it is necessary for federal laws to be enacted to ensure the citizens of this entire country are afforded the protections set forth in the Constitution of this great nation.\(^{84}\) While trends are showing 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.

\(^{83}\) See, Hudson, supra note 60 (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); supra note 10.

\(^{84}\) U.S. Const. amend. IV (The Fourth Amendment provides “[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.”); Hudson, supra note 60 (Attorney Bradely Shear discusses the fact that there is neither a federal law or a Supreme Court decision that speaks to this issue, therefore, “…new laws are needed to clarify the legal landscape.”)
Thankfully, this matter seems to be getting more and more attention and it may a welcomed indication that what has been growing into the norm—invading people’s privacy—will be thwarted, allowing the tides to turn, and a the shift will be for this new legislation to establish a mandate of what will not remain the trend for the schools and employers.  

In April 2012, State Representative, Elito Engel, introduced the Social Networking Online Protection Act (SNOPA), which is also known as House Resolution 5050. 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. Specifically, it would be unlawful for an employer to require an employee or applicant for employment provide a username, password, or any credential information that would gain the employer’s access to electronic media tied to the applicant, including e-mail accounts, personal accounts on social networking sites. In addition, it would be unlawful to discriminate against, deny employment, or threaten action against any an applicant who declined to provide their online credentials. The bill is also thorough in that it includes an anti-retaliation provision prohibiting action to be taken against an applicant for filing a complaint or participating in activities related to reporting a violation of this Act. It is also important to note that the Act considers an “employer” to be

---

85 *Id.* (Attorney Bradely 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.”)

86 2011 CONG US HR 5050, 112th CONGRESS, 2nd Session

87 *Id.*

88 2011 CONG US HR 5050, 112th CONGRESS, 2nd Session
“any person acting directly or indirectly in the interest of an employer in relation to an employee or an applicant for employment.” 89 In addition, SNOPA also specifically provides for protection to existing employees, but these protections have not been outlined in this note since that was not the focus of this discussion. Should an employer violate the proposed law, it would for a civil penalty of up to ten thousand dollars. It also would authorize the secretary of labor to seek injunctive relief to restrain violations and require compliance. 90 Moreover, the will would grant the federal courts with jurisdiction to issue appropriate relief. 91

Similarly, SNOPA would also serve to cover some of the children and students of educational organizations who has also been left out to dry by some of the relatively new state laws that have been enacted. 92 SNOPA would also prevent some educational intuitions and local 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 to. 93

Shortly after the introduction of SNOPA, the Password Protection Act of 2012 (PPA), S.3074 and H.R. 5684, was also introduced in the House and Senate. 94 Like SNOPA, the

---

89 2011 CONG US HR 5050, 112th CONGRESS, 2nd Session; see also Tamara R. Jones, SNOPA PROPOSED TO PROHIBIT SNOOPING 23 No. 9 Tex. Emp. L. Letter 3, September 2012.
90 See Tamara R. Jones, SNOPA PROPOSED TO PROHIBIT SNOOPING 23 No. 9 Tex. Emp. L. Letter 3, September 2012.
91 Id.
92 2011 CONG US HR 5050, 112th CONGRESS, 2nd Session
93 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).
94 Leslie Hayes, Sally J. Cooley, Article, Social Media-Striking the Balance Between Employer and Employee, 55 DEC Advocate (Idaho) 22 (Nov./Dec. 2012).
proposed legislation would also prohibit employers from demanding a person give access to their social networking accounts.\textsuperscript{95} The PPA would serve to amend current law.\textsuperscript{96}

**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 face absent new laws to address the ever changing technology landscape. While it should provide comfort that the 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. From young to old, the Constitution affords citizens of this country protection and it has been interpreted to preserve a right to privacy. As this note demonstrates, the intent of this precious amendment is being eroded with each day that passes. Therefore, passage of SNOPA and PPA is the most uniform way to ensure that all people are afforded equal protection and to ensure varying language from state to state does not preclude individuals from employment or educational advancements simply because of a snooping eye.

V. Conclusion

Regardless of what side of the issue you stand on—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 purpose they serve. Just as individuals whose right to privacy is being established if the Act is signed into law; school organizations and employers, so too, should also be aware of

\textsuperscript{95} Id.
\textsuperscript{96} Id.
the benefits it brings.

First, it clearly establishes the lines you can and cannot cross. Secondly, you do not expose yourself to unintended litigation. As the old adage says, “avoid the appearance of evil,” SNOPA and the PPA assists by ensuring your organization cannot engage in activity that can give the appearance of using hiring or admission decisions that were, in part, based on protected criteria, such as race, age, religion, 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, giving the judicial branch a clear basis to interpret and uphold the law as it was intended. Furthermore, this law will mitigate the risk of relying on otherwise ambiguous law, which creates splits among many circuits, and ever clogging the docket. To date, case law has demonstrated the challenges the various state courts have faced with attempting to interpret outdated language of the various technology related laws and the great difficulty in determining just how the recent developments in technology impacts the rights of each party to the litigation.

But above all else—each of us are individuals—whether by day we sit on the side of the table that is demanding the social media credentials or not—once you leave work—you too, are just an individual. 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 as well. Whether we apply the Golden Rule Principal, Utilitarian, or the Kantian principle, it certainly seems from both a legal and ethical perspective, protecting personal privacy is treating someone else
as we would expect to be treated, it is what will promote the greatest happiness for all, and ensure we do not use each other as just a means; rather we both are in the position to consent to transact with each other in a harmonious manner (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 that it really mean for you, your family, and your friends. 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’ your job, job offer, acceptance, or admittance? Are you okay 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.