WHAT ARE YOU LOOKING AT?:
WHY THE PRIVATE SECTOR’S USE OF
SOCIAL MEDIA NEED NOT BE LEGISLATED

By Courteney B. Lario*

I. INTRODUCTION ................................................................. 134
II. BACKGROUND ................................................................. 137
   A. History of Social Network Sites ......................................... 137
   B. Controversies Leading to Legislation .................................. 138
   C. Legislative Overview ..................................................... 141
   D. Enforcement Techniques ............................................... 143
   E. Goals Behind Legislation ................................................. 145
III. PROBLEMS WITH LEGISLATION .......................................... 146
   A. Difficulty of Enforcement ............................................... 146
   B. Preemptive Legislation .................................................. 150
   C. Employers’ Disincentives ............................................... 153
IV. ANALYSIS ................................................................. 156
   A. Setting the Stage for Legislative Ineffectiveness ...................... 157
   B. Public Sector versus Private Sector Legislative Oversight ............ 160
V. CONCLUSION .................................................................. 161

* J.D. Candidate, 2014, Seton Hall University School of Law; B.A. in Government and English, Georgetown University, 2011. I would like to thank Professor Charles Sullivan and Wendy Johnson Lario for all their help and guidance on this Note.
I. INTRODUCTION

“Employers have no right to ask job applicants for their house keys or to read their diaries—why should they be able to ask them for their Facebook passwords and gain unwarranted access to a trove of private information about what we like, what messages we send to people, or who we are friends with?” commented Senator Charles Schumer of New York.1 This sentiment regarding online privacy is popular among legislators, with bills introduced in at least forty state legislatures as well as the United States Congress over the past two years aimed at protecting employees or job applicants from employers requesting access to passwords of social media websites.2 The current movement toward preventing employers from requesting passwords for social media websites arose primarily after controversies developed surrounding state governments requiring job applicants’ passwords.3 The first of these stories involved a governmental entity in Maryland demanding a job applicant’s Facebook password in 2011.4 Maryland soon thereafter became the first state to propose and pass a bill banning employers from accessing social media passwords. This bill went into effect in October 2012.5 After several similar stories cropped up across the country, more states began proposing and enacting similar laws. Six of the forty states that proposed such legislation, California, Delaware, Illinois, Maryland, Michigan, and New Jersey, successfully enacted privacy laws in 2012.6 And, an additional eight states passed laws

---

2 National Conference of State Legislatures, Employer Access to Social Media Usernames and Passwords 2013 (2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords2013.aspx. These numbers are those at the time of publication. This number represents the current number of state legislatures that have proposed this bill as of December 31, 2013.
4 Id.
5 Id.; Md. CODE ANN., LAB. & EMP. § 3-712 (West 2012). See discussion infra Part I.B.
2013] WHAT ARE YOU LOOKING AT? 135

relating to social media policies in 2013.\(^7\)

Although an ever-increasing number of stories are published regarding employers demanding Facebook passwords, questions remain as to the actual extent of the practice and the necessity for such laws at this time.\(^8\) Several key issues underscore the questionable utility of these laws. First, with no defined administrative mechanism or specific execution provision, the laws themselves are difficult to enforce. Second, the acts are preemptive and lack substantive facts or figures to warrant their passage. Third, employers already have incentives to not request access to an employee’s online information in order to protect themselves from discrimination, privacy, and other labor and employment-related lawsuits. Additionally, these laws are not necessary to protect the employees or applicants who are asked for online usernames and passwords and are later fired or not hired based on social media information. This is because employees and applicants have other well-established means of protection such as: privacy torts, Title VII of the Civil Rights Act (“Title VII”), and the First Amendment.\(^9\) Despite these concerns, state legislatures continue to propose and easily pass laws as an attempt to protect employees and job applicants.

Many of the local state governments are actually the primary culprits in creating online privacy issues through the hiring process.\(^10\) State legislatures, rather than passing wide-reaching and unnecessary laws, should take the opportunity to enact legislation that regulates

---


\(^10\) See discussion infra Part I.B.
their own state and local agencies’ employment policies.\textsuperscript{11} Private-sector employers, who are guided by the legal risks and exposures that come with employment decisions when using social media in the hiring and firing processes, should be permitted to handle these matters themselves.\textsuperscript{12} Because public and private sector employers have different methods, obligations, and risks associated with employment decisions, legislatures should not over-legislate and restrict the hiring and firing practices of all employers in online privacy acts.\textsuperscript{13}

This Note addresses the new legislative measures designed to protect employees’ and applicants’ online privacy, and highlights some of the concerns about the passage of these acts. The Note proceeds in three stages. Part I addresses the background of the various state and federal legislative proposals. Part I also reviews the history and reasoning behind the legislative efforts, and dissect the laws themselves. Part II considers three concerns regarding the necessity of these laws. The first concern is the question of enforceability. The second concern focuses on the lack of evidence justifying these laws in the private sector. The third concern regarding these types of legislation is the absence of any legal need to impose regulations on private sector employers that are already protecting themselves from lawsuits by not requiring or even requesting online information from its employees or applicants. After addressing those primary concerns regarding the necessity of these laws, Part III analyzes how those three issues should affect the passage of the legislation. Finally, this Note concludes that state and federal


\textsuperscript{12} Anna Hickman, Don’t Bother Asking for Facebook Passwords, 27 CORP. COUNS’OR. 7, 9 (Aug. 16, 2012).

\textsuperscript{13} Joe Weisenthal, The Public Sector vs. The Private Sector in One Colossal Chart, http://www.businessinsider.com/chart-the-public-vs-private-sector-20127; Allison, supra note 11, at 14. These articles show that the private sector is much more financially stable and successful than the public sector. Additionally, there is a stark difference in managerial authority between the public and private sector. “The general management functions concentrated in the CEO of a private business are, by constitutional design, spread in the public sector among a number of competing institutions and thus shared by a number of individuals whose ambitions are set against one another.” Allison, supra note 11, at 21.
legislatures, rather than addressing both public and private sector employers, should instead limit such legislation to only the public sector. There is not yet a need for laws regarding online privacy information beyond the public sector because other concerns outweigh the need for regulation in this area.

II. BACKGROUND

This section addresses the background and history leading up to the proposal of legislation limiting access to employees’ and applicants’ online information. Specifically, this section highlights the controversies publicized by the media that drew attention to and served as the catalyst for these legislative measures. This section also details the actual legislation in states that passed limiting laws, the states that proposed similar laws, and the proposed federal bills. Lastly, this section provides an overview of the goals and reasoning behind the proposed legislation.

A. History of Social Network Sites

For this Note, social network sites are defined as “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.” The key to a social network site is that individuals have public and visible social network profiles or information that is shared with that individual’s “friends,” who are other users of that social network identified as having a relationship with that specific individual. Generally, this Note combines these various social networking sites under the term “social media.”

The first known and recognized social network website was SixDegrees. SixDegrees.com launched in 1997 and allowed users to “create profiles, list their Friends, and... surf the Friends list.”

---

15 Id. at 213. “Friends” can be identified with different labels depending on the social network site. Id.
16 Id. at 214.
17 Id.
SixDegrees aimed to connect people online by allowing individuals to send messages to one another.\textsuperscript{18} Though several more social networking sites were launched over the next few years, a large burst of them came in 2003 with the creations of LinkedIn and MySpace.\textsuperscript{19} Facebook began the following year as a Harvard student-only social network site.\textsuperscript{20} Facebook next opened up to other university students in 2005, just as YouTube launched its video-based site.\textsuperscript{21} While Facebook expanded to allow access to nearly anyone with an email address in 2006, Twitter also arrived onto the worldwide social network scene.\textsuperscript{22}

\textbf{B. Controversies Leading to Legislation}

Before state legislatures and Congress proposed laws banning employers from requesting social media passwords from job applicants, several publicized controversies led to the demand for these legislative measures. The first major issue occurred in Maryland in 2011.\textsuperscript{23} There, the Maryland Department of Public Safety and Correctional Services required that a corrections officer in his recertification process provide his Facebook password, supposedly to determine whether the officer had ties to gang members.\textsuperscript{24} The American Civil Liberties Union ("ACLU") of Maryland took a stance against this new practice in a press release issued in February 2011.\textsuperscript{25} The ACLU also posted a YouTube video highlighting the story and requesting that the Department no longer demand online passwords.\textsuperscript{26} In response to the public outcry, the Department

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{18}] Id.
\item[\textsuperscript{19}] Id. at 216.
\item[\textsuperscript{20}] Boyd & Ellison, supra note 14.
\item[\textsuperscript{21}] Id. at 218.
\item[\textsuperscript{22}] Id.
\item[\textsuperscript{23}] Bernabei & Kabat, supra note 3, at 42.
\item[\textsuperscript{24}] Id.
\item[\textsuperscript{26}] Aaron C. Davis, Maryland corrections department suspends Facebook policy for prospective hires, WASH. POST. (Feb. 22, 2011, 9:58 PM), available at http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207486.html.
\end{itemize}
\end{footnotesize}
temporarily suspended the practice. Nevertheless, soon thereafter in May 2012, Maryland Governor Martin O’Malley signed into law the User Name and Password Privacy Protection Act, proposed and passed by the Maryland legislature. This law was the first of its kind and marked the beginning of a nationwide trend.

A second controversy occurred in Bozeman, Montana, in 2009, when the city government required all job applicants to provide usernames and passwords for social media sites, including Facebook, Google, Yahoo, MySpace, and YouTube. In June 2009, the city manager of Bozeman issued a statement suspending the city’s requirement but only after the city government received numerous complaints from its citizens about this practice. Ultimately, on February 27, 2013, Montana’s state Senate passed a bill protecting private electronic information of job applicants and employees. The Montana social media password privacy bill is currently awaiting a vote in the state House of Representatives.

A third controversy arose in Minnesota when a young female student announced that her public school demanded she provide her login information to Facebook and email accounts. The student said that the school asked for her passwords following allegations that she was having conversations about sex with another student. Supposedly, the school administrator informed the student that she

---

27 Id.
29 National Conference of State Legislatures (2012), supra note 6.
32 S.B. 195, 63d Leg. (Mont. 2013).
33 Id.; National Conference of State Legislatures (2012), supra note 6.
35 Id.
would be punished if she did not provide the information. The ACLU of Minnesota filed a lawsuit in 2012 against the student’s school district, the Minnewaska Area Schools, as well as the Pope County Sheriff’s office for violating the constitutional rights of the minor student. Specifically, the ACLU argued that public entities violated the girl’s First Amendment right to free speech for off-campus behavior and her Fourth Amendment right to be free from unreasonable search and seizures. Subsequently, Minnesota’s state legislature proposed social media legislation in 2012, which is still pending.

Aside from the issues that arose following state or local government actions, there has also been a general trend in the federal government hiring policy requiring more detailed and in-depth information for job applicants. President Barack Obama created a more comprehensive vetting process for high-ranking executive branch applicants than his predecessors, which includes requiring disclosure of any “email(s) that might embarrass the president-elect, along with any blog posts and links to their Facebook pages.” Although the executive branch application did not require applicants to relay their username or passwords for social media websites, it did require information regarding private Internet posts

---

36 Id.
37 The school district and sheriff’s office moved to dismiss, arguing that they did not violate the Constitution. The U.S. District Court for the District of Minnesota denied the motion to dismiss, holding that the girl’s constitutional rights were established and the defendants’ conduct could amount to violations. However, the Court also found that “certain claims advanced by the Plaintiffs—civil conspiracy to deprive [the minor] of her civil rights and intentional infliction of emotional distress—have not been sufficiently pled,” and were thus dismissed, R.S. ex rel. S.S. v. Minnewaska Area School District, No. 2149, 894 F.Supp.2d 1128, 1133 (D. Minn. 2012).
40 See generally Jackie Calmes, For a Washington Job, Be Prepared to Tell All, N.Y. TIMES, (Nov. 13, 2008), available at http://www.nytimes.com/2008/11/13/us/politics/13apply.html?_r=2& (discussing President Barack Obama’s sevenpage questionnaire, which included 63 requests for personal and professional records, for high-ranking applicants for the President’s first administration).
41 Id.
or emails. Thus, the federal government created a standard of all-encompassing application inquiries, including information from new forms of online data.

Each of the aforementioned situations arose out of requirements for information from a governmental entity. Each employer indicated that it asked for usernames and passwords to serve as a background check or guard against inappropriate behavior. “Before we offer people employment in a public trust position, we have a responsibility to do a thorough background check,” said Chuck Winn, Bozeman, Montana’s assistant city manager, when originally interviewed about the city’s application requirements. Despite the trend toward government transparency, these acts raise some questions as to whether the requests are going too far. Thus, in reaction to these issues, especially after the Maryland story, state legislators decided it was time to take action.

C. Legislative Overview

As of the writing of this article, at least forty state legislatures have now proposed or passed legislation banning access to social media passwords. Congress has also proposed legislation of this kind. In 2012, six states enacted legislation that prohibits employers and/or schools from requesting an employee, student, or applicant to disclose private online information—California, Delaware, Illinois, Maryland, Michigan, and New Jersey. Eight other states proposed

---

42 Id.
43 Id.
44 See discussion supra Part I.B.
45 McCullagh, supra note 30.
46 Calmes, supra note 40.
48 Id.
online privacy legislation in 2012: Massachusetts, Minnesota, Missouri, New York, Ohio, Pennsylvania, South Carolina, and Washington. An additional twenty-six states proposed laws in 2013: Arizona, Arkansas, Colorado, Connecticut, Florida, Georgia, Hawaii, Iowa, Kansas, Louisiana, Maine, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Carolina, North Dakota, Oregon, Rhode Island, Texas, Utah, Vermont, West Virginia, and Wisconsin. Thus far, eight of these states have passed their acts in 2013.

Two separate acts were proposed in Congress in April 2012: H.R. 5684, the Password Protection Act of 2012, and H.R. 537, the Social Networking Online Protection Act. The Password Protection Act would prohibit employers from requiring job applicants and employees to provide access to their private online accounts. This act would apply to employers’ use of any online password information.

---


as a condition of employment, discrimination, or retaliation. The Password Protection Act would be integrated into the Computer Fraud and Abuse Act, which was an act “passed by Congress in 1984 to address the unauthorized access and use of computers and computer networks.” The Social Networking Online Protection Act, on the other hand, would prohibit employers and schools from requiring or requesting that employees, students, and job applicants provide a username or password to access a personal account on any social networking website. This act would create a stand-alone new law limiting access to private online information, rather than one combined with the Computer Fraud and Abuse Act.

D. Enforcement Techniques

Of the fourteen states that have passed legislation banning access to online information, seven specifically ban both employers and institutions of education from “requesting or requiring” any usernames or passwords to online information. Five states passed bills that ban only employers from requesting usernames or passwords to social media sites. Delaware passed an act that banned only academic institutions from requiring online password information. Finally, Vermont passed a law that sets up a committee to “study the issue of prohibiting employers from requiring employees or applicants for employment to disclose a means of accessing the employee’s or applicant’s social network account.”

58 H.R. 537 113th Cong. (2013); Hirschfeld & Oliveira, supra note 9.
Of these fourteen laws, only six of them have specified means of enforcing an employer’s or school’s actions.\textsuperscript{64} Utah’s Internet Privacy Amendments and Washington’s Employment Security, Privacy for Social Networking Accounts Act provide that an aggrieved individual may bring a civil cause of action, in which the court shall not award that individual with more than $500.\textsuperscript{65} Similarly, Michigan’s Internet Privacy Protection Act provides that an individual can bring a civil suit and may recover not more than $1,000 in damages, with any reasonable attorney fees and court costs.\textsuperscript{66} However, Michigan’s Act also provides that a person who violates this Act is guilty of a misdemeanor.\textsuperscript{67} Therefore, Michigan’s Act takes a step further than Utah’s and makes a violation a criminal action.\textsuperscript{68}

New Jersey and Nevada’s laws, unlike the acts above, allow for an aggrieved individual to make claims against the employer or institution.\textsuperscript{69} However, New Jersey’s does not include a specific amount of costs, but rather indicates that an individual is entitled to injunctive relief, compensatory and consequential damages, plus reasonable attorney fees and court costs.\textsuperscript{70} Nevada’s statute allows an individual to recover legal or equitable relief, such as “reinstatement of the employee’s position and the payment of lost wages and benefits.”\textsuperscript{71} Nevada also provides for an administrative penalty by the Labor Commissioner of not more than $9,000 for each violation of the act.\textsuperscript{72}

When it comes to enforcement provisions of the federal bills,
both bills include more stringent and severe violation penalties.\textsuperscript{23} Since the Password Protection Act would be interwoven with the Computer Fraud and Abuse Act, enforcement provisions already exist.\textsuperscript{74} There are several penalties in the Computer Fraud and Abuse Act depending on the violation, including both fines and imprisonment from one to twenty years.\textsuperscript{25} The Social Networking Online Protection Act, on the other hand, is very clear that its remedy is a civil violation that is actionable by the Secretary of Labor.\textsuperscript{76} Additionally, an employer that violates the Social Networking Online Protection Act can pay a fine of no more than $10,000.\textsuperscript{77} Therefore, the two federal acts include provisions for harsher penalties and would allow for stricter enforcement via civil suit and the Secretary of Labor.\textsuperscript{78}

\textit{E. Goals Behind Legislation}

Each of the proposed bills or enacted statutes provides some restrictions against employers requesting employees' or applicants' online passwords.\textsuperscript{79}

[T]his legislation prohibits employers or schools from requiring employees, students or applicants to disclose their social-media passwords, or otherwise to provide access to private material on social-media Web sites. These legislative efforts also prohibit taking adverse actions against individuals who refuse to disclose their passwords.\textsuperscript{80} Generally, employers are not able to gain non-workspace information without an employee's consent.\textsuperscript{81} The legislators do not seem to be convinced by the arguments that by gaining access to these personal accounts the employer is merely doing its due diligence and protecting itself against incompetence, negligent hiring lawsuits, and

\begin{flushright}
\textsuperscript{23} H.R. 5684; H.R. 537.
\textsuperscript{25} \textit{Id}.
\textsuperscript{74} Id.
\textsuperscript{75} H.R. 537.
\textsuperscript{76} \textit{Id}.
\textsuperscript{77} Id.
\textsuperscript{78} H.R. 5684; H.R. 537.
\textsuperscript{79} Bernabei & Kabat, \textit{supranote} 3, at 42.
\textsuperscript{80} \textit{Id}.
\textsuperscript{81} \textit{Id}.
\end{flushright}
resume fraud.\textsuperscript{82} Where the bills have been successful, the state legislatures seek to protect employees from these password requests, in addition to providing a remedy in case the law is not followed.\textsuperscript{83}

\textbf{III. PROBLEMS WITH LEGISLATION}

This section of the Note presents arguments as to why state and Congressional efforts to ban the practice of requesting online and social media passwords are not necessary. The first reason is that the aforementioned bills— and undoubtedly copycat bills to come— are difficult to enforce without a distinct implementation mechanism and an assortment of remedies. Second, the legislatures are preemptively passing acts without proof of their actual necessity because there is no clear proof of how many employers or government bodies are requesting these passwords. Additionally, there are not enough studies or statistics to glean the number of applicants affected by these password requests. Third, employers already have legal reasons to avoid seeking password-protected information— to protect themselves against lawsuits or legal claims. Employees or applicants, who are required to provide social media access and then fired or not hired, have means to protect themselves, including bringing a claim of invasion of privacy or discrimination against the employer. Thus, because an employer puts itself at risk for a lawsuit when requiring social media passwords, the passage of these acts is merely a further disincentive for employers to do something most are already avoiding.

\textbf{A. Difficulty of Enforcement}

An initial reason that laws banning employers from requesting an applicant’s social media passwords are ineffective is the difficulty of enforcement.\textsuperscript{84} There are several reasons why this legislation is difficult to enforce: (1) varying enforcement mechanisms are creating uncertainty among the different state and congressional bills; (2) infeasibility of monitoring employers or governments; (3) lack of financing for enforcement agency or function; and (4) the

\begin{flushleft}
\textsuperscript{82} Hirschfeld & Oliveira, \textit{supra} note 9.
\textsuperscript{83} See generally \textit{id}.
\textsuperscript{84} Bernabei & Kabat, \textit{supra} note 3, at 42.
\end{flushleft}
government’s enforcement power over the employer outside the public sector is uncertain.\textsuperscript{85}

A major problem with enforcement is that many of the current bills have differing enforcement mechanisms or are lacking them altogether.\textsuperscript{86} Bills from different states provide assorted enforcement actions, as discussed above.\textsuperscript{87} While some states, such as New Jersey and Utah, provide private civil rights of action, other states, such as Michigan, create a misdemeanor offense in addition to the civil and administrative remedies.\textsuperscript{88} Additionally, Utah and Michigan provide limited damages that a court can award to an aggrieved claimant, while New Jersey sets no specific damage limit.\textsuperscript{89} On the other hand, the bills proposed in other states, such as California, Maryland, Missouri, and South Carolina, provide no enforcement mechanism whatsoever.\textsuperscript{90} In those states, an individual could presumably bring a tort claim “for wrongful discharge in violation of public policy” and could use this legislation as the public policy basis.\textsuperscript{91} In that case, individuals would then have a full range of remedies available.\textsuperscript{92} These varying enforcement measures make it difficult for national employers to create and defend regulations for the company as a whole. For example, in Michigan, an employer may face criminal charges, while in Utah, an employer only has to pay a fine of up to $500.\textsuperscript{93}

In addition, the federal government would have difficulty enforcing the proposed congressional social media bills.\textsuperscript{94} Specifically,

\begin{itemize}
\item \textsuperscript{85} See discussion infra Part II.A.
\item \textsuperscript{86} See discussion supra Part I.C.
\item \textsuperscript{87} \textit{Id}.
\item \textsuperscript{91} Bernabei & Kabat, supra note 3, at 42.
\item \textsuperscript{92} \textit{Id}.
\item \textsuperscript{94} H.R. 5684, 112th Cong. (2012); H.R. 537, 113th Cong. (2013).
\end{itemize}
the Social Networking Online Protection Act “allows for enforcement only through the U.S. Department of Labor [(“DOL”)], at a time when that agency lacks the resources to enforce other federal employment statutes.”\textsuperscript{95} The United States has embraced an ideal that the Internet should primarily be self-regulated.\textsuperscript{96} Thus, the United States does not have a regulatory body for invasions of privacy when it comes to online information.\textsuperscript{97} Additionally, the DOL, a department that could regulate this act federally, already “administers and enforces more than 180 federal laws.”\textsuperscript{98} In a 2006 Performance and Accountability Report (“PAR”), the DOL assessed twenty-eight of its programs to determine each programs’ effectiveness.\textsuperscript{99} Out of the twenty-eight programs reviewed under the PAR, DOL rated one “effective,” eight “moderately effective,” deemed twelve “adequate,” and ranked the last four “ineffective.”\textsuperscript{100} The DOL has also specifically admitted to ineffectively enforcing certain acts in the past.\textsuperscript{101} Therefore, it is nearly impossible for the government to regulate, watch, and monitor every employer in a certain jurisdiction with the DOL admittedly performing “adequately” in a majority of areas.\textsuperscript{102}

In addition, unlike in many of the state causes of action, the Social Networking Online Protection Act only allows the Secretary of Labor to bring an action, while most states allow only for private civil

\textsuperscript{95} Bernabei & Kabat, supra note 3, at 42; Kenneth Kopelman, Closing the Courthouse Door on Section 503 Complaints; Davis v. United Air Lines, Inc., 49 BROOK. L. REV. 1159, 117677 (1983).

\textsuperscript{96} See generally Ryan Moshell, .... And then there was one: The outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection, 37 TEX. TECH. L. REV. 359 (2005) (discussing how the United States should develop a more comprehensive data protection regime); Milton Mueller, ICANN and Internet Governance: Sorting Through the Debris of Self-Regulation, 1 J. POLY RED. STRATEGY FOR TELECOMM. INFO. MEDIA, 497 (Dec. 1999), available at http://www.icannwatch.org/archive/mueller_icann_and_internet_governance.pdf.

\textsuperscript{97} Moshell, supra note 96, at 367.


\textsuperscript{100} Id. at 49-50.

\textsuperscript{101} Kopelman, supra note 95, at 117677.

causes of action. This confusion again leads to difficulty for large national companies that span several or all states because that company could get sued by an individual in one state and pay a minimum fine, and later get sued by the Secretary of Labor and pay a much larger fine. In turn, the Password Protection Act, as mentioned above, which would amend the Computer Fraud and Abuse Act, provides both civil and criminal means of enforcement. This creates a further problem, however, because the Computer Fraud and Abuse Act covers a wide array of computer violations, and where the new amendment would fit in is unclear, specifically in regard to the enforcement section.

A third major issue with enforcement is funding. In the economic circumstances that the United States now faces, the government is looking for measures to cut spending. "There surely are more economic shocks in store, including increased unemployment, more corporate defaults, and state and local government budget emergencies." Funding to create jobs or a new government entity to oversee employers pursuant to this new legislation would actually create a buildup of resources and spending in the public sector because enforcement and enactment would be so confusing and ineffective. However, over the past year, local, state, and federal government jobs have dropped by 162,800 jobs, a .7 percent decline. With declining job numbers in the government sector and a goal to cut government spending, including a recent sequester, neither state nor federal governments have money or manpower left to create an entity or pay more employees to monitor employers and their online information usage.

105 Id.
108 Id. at 10.
110 See id.
Combining the reasoning above, the recent legislative measures attempting to ban employers from requiring access to employees’ or applicants’ social media passwords are, overall, difficult to enforce. The variability amongst the state and federal acts, the infeasibility of enforcement, the lack of funds needed to enforce these laws, and the question as to whether it should be the government’s responsibility to monitor these employers led to the impracticability of implementing these laws, both administratively and functionally.\textsuperscript{115}

\textbf{B. Preemptive Legislation}

Many of the controversies surrounding the password requests occurred in state government entities.\textsuperscript{112} But, rather than the states handling these issues with state government policy changes, specifically through hiring policies, the states decided to legislate against these practices in both the public and private sectors.\textsuperscript{113} Beyond the proof of the state or local government social media use, there is, moreover, reason to doubt that many companies, employers, or schools are requesting online passwords.\textsuperscript{114} Shel Israel, of Forbes states:

\textquote{T}here is real question as to how widespread such practices really are. The number of cases reported so far appears to have three aspects in common: 1. They involve government positions, most of them public safety jobs. This does not justify the privacy invasion, but may explain overreaction by employers who really do need to worry about security. 2. All incidents being reported are more than a year old. 3. As far as I could find, there is not a single report of passwords being demanded by private sector companies.\textsuperscript{115}

In his article, Israel argues that these online privacy bills are proposed without any proof as to how many people are affected.\textsuperscript{116} Specifically, he states that this is a non-issue that has been turned into a large concern only because of the local government issues and

\begin{footnotes}
\footnote{\textit{Sec}discuss\textit{ion supra, Part II.A.}}
\footnote{\textit{See} Bernabei & Kabat, \textit{supra note} 3; \textit{see also}, discussion \textit{supra Part II.A.}}
\footnote{Bernabei & Kabat, \textit{supra note} 3.}
\footnote{Israel, \textit{supra note} 8.}
\footnote{\textit{Id.}}
\footnote{\textit{Id.}}
\end{footnotes}
Though there are not many statistics, or much evidence, revealing how many employers are requiring passwords or how many applicants are affected by this practice, there are some indicators that point to a lack of any problem regarding access to private online accounts, especially within the private sector. In Senator Schumer’s press release asking the U.S. Equal Employment Opportunity Commission (“EEOC”) and the U.S. Department of Justice (“DOJ”) to investigate the recent activity of employers requiring online passwords, he cited “recent reports” showing that “some” employers were requiring disclosure of passwords. The “recent reports” that the press release makes reference to consist of three media stories based on individual narratives.

In one case, the Associated Press reported a New York City statistician was asked for his Facebook username and password so that the employer could review private components of his profile as part of the interview process for the job he was applying for. At least two other cases were identified where individuals who were applying for jobs were required to turn over Facebook passwords and usernames in order to be considered for the job they were applying for, as well as a city that, until recently, required job applicants to provide access to their email accounts.

These three accounts were the only factual bases used for Senator Schumer’s report regarding the practice of requesting or requiring online passwords in New York.

In fact, when it comes to available statistics regarding how many employers are requiring an online password, there are not many studies in existence. However, Littler Mendelson, P.C. completed one poll of over 1,000 high-level companies, which showed that fewer than one percent of the companies surveyed had “requested social media logins as part of the hiring or onboarding process.”

---

117 Id.
118 See Press Release, Senator Charles Schumer, supra note 1.
119 Id.
120 Id.
121 Id.
this does not cover all companies, it strongly suggests that almost none of the most successful private sector entities are requesting social media passwords.\textsuperscript{123}

However, this is not the first time that legislation has been enacted to deal with a supposed problem without statistics or evidence to document the existence of the problem in the first place.\textsuperscript{124} In 2008, Congress preemptively passed the Genetic Information Nondiscrimination Act (“GINA”) in order to prohibit employers from discriminating against employees or applicants based on genetic information.\textsuperscript{125} Some in opposition to this act said that there was no proof that any such discrimination was occurring and that discrimination based on genetic information is rare.\textsuperscript{126} In passing the bill, Congress relied primarily on three individual examples of genetic discrimination, all of which arguably could have relied on relief claims under Title VII or the American with Disabilities Act.\textsuperscript{127} Therefore, it seems Congress preemptively passed GINA without solid statistics or any strong evidence in support of the Act.\textsuperscript{128}

Although GINA protects against possible discrimination based on genetic information, there are some downsides of GINA having

\textsuperscript{123} See generally id.


\textsuperscript{127} Roberts, supra note 124, at 465-66.

\textsuperscript{128} \textit{Id}. 
2013] WHAT ARE YOU LOOKING AT? 153

been preemptively passed. Another negative is that it is nearly impossible to measure the Act’s effectiveness without prior statistics. Discovering whether the legislation has actually protected anyone is nearly impossible. Another consequence of Congress passing GINA preemptively is that GINA “may fail to alleviate (or may even legitimize) fears of genetic-information discrimination.” Because Congress passed GINA before genetic discrimination affected many people, it seems possible that GINA raises more awareness about genetic discrimination than is desirable. In doing so, it generates fears of discrimination that did not previously exist. Rather than protecting and assuaging individuals’ fears, it creates and stimulates the necessity of that fear.

GINA provides a comparison for the legislation banning employers from requesting social media passwords at both the state and congressional levels. Like GINA, this recent password legislation does not have much empirical evidence, and relies heavily on anecdotal personal stories. Without much data the password legislation seems also to be preemptive, and thus encounters those same problems that GINA does. Typically, in the past, discriminatory legislation was passed retroactively.

C. Employers’ Disincentives

Employers open themselves up to lawsuits by looking into online information, particularly when viewing private personal information. Specifically, employees or applicants could bring suit against the employer for using private information in the hiring or firing process on various bases, including religion, sexual orientation, disability, or marital status. If an applicant is not hired after

---

129 Id. at 490.
130 Id.
131 Id.
132 Id.
133 See Roberts, supra note 124, at 465-66.
134 Id.
135 Id. at 490.
136 Id.
137 Id. at 457.
138 Hickman, supra note 12, at 2.
139 Hirschfeld & Oliveira, supra note 9, at 1.
providing social media access, that applicant can later claim that said information was the reason. These employers, who review online information or require social media passwords, expose themselves to claims ranging from discrimination and retaliation to constitutional or tort-based privacy issues. For example, Title VII states that it is unlawful for an employer to discriminate based on race, color, religion, sex, or national origin. The First Amendment also protects freedom of speech and freedom of religion. In addition, one of the four torts that falls under the rubric of invasion of privacy is intrusion upon seclusion, which addresses acts of intrusion into a victim’s zone of privacy.

There have been several examples of employers not hiring a job applicant and that applicant then raising a claim of discrimination because of discovered online information. While such cases do not arise specifically from employers requesting private passwords, they do involve employers discovering an applicant or employee’s personal information from online resources.

Gaskell v. University of Kentucky involves a discrimination claim under Title VII. In that case, Gaskell alleged that the university rejected him after the hiring committee found information on his religious views during an Internet search. In the end, the judge denied cross-motions for summary judgment, and the case would have proceeded to further trial if it had not settled for $125,000.

---

10. Id.
11. See generally, id.
14. RESTATEMENT (SECOND) OF TORTS § 652B (1977). Though a victim has not yet used this invasion of a zone of privacy in the online spectrum of personal and social media information, it is one of the avenues that could have been tested prior to the passage of this legislation.
15. See Wagner v. Jones, 664 F.3d 259 (8th Cir. 2011); Gaskell v. Univ. of Kentucky, No. 09-244, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010).
16. See Wagner, 664 F.3d at 264; see also Gaskell, 2010 WL 4867630, at *4.
17. See generally, Gaskell, 2010 WL 4867630.
18. Id. at *4.
19. Id. at *1; A Reminder to Hiring Committees: Don’t Google the Candidates?, PRAWFSBLAWG (Aug. 29, 2012), http://prawfsblawgblogs.com/prawfsblawg/getting_a_job_on_the_law_teaching_market/.
Although this case settled, it reveals that a triable issue of fact can exist in a discrimination claim predicated on discovered online information.\textsuperscript{150} And though this case does not involve requesting online passwords, it shows that even a basic Internet search exposed the employer to liability based on the information discovered.\textsuperscript{151} Accordingly, an employee or applicant could raise a discrimination claim under Title VII, the Age Discrimination in Employment Act, or the Americans with Disabilities Act from information discovered during a search using their personal passwords.\textsuperscript{152}

A second example is Wagner \textit{v.} Jones, which involved the University of Iowa College of Law and its failure to hire a writing instructor whose political beliefs were available online.\textsuperscript{153} In the end, the court found that Wagner, the applicant, had presented enough evidence of discrimination that the case could be brought to a jury.\textsuperscript{154} On appeal, the Eighth Circuit applied the following test for discrimination:

In political discrimination cases, nonpolicymaking employees have the threshold burden to produce sufficient direct or circumstantial evidence from which a rational jury could find that political affiliation was a substantial or motivating factor behind the adverse employment action. At that point the employer must articulate a nondiscriminatory basis for the adverse employment action and prove by a preponderance of the evidence that it would have been taken without regard to plaintiff’s political affiliation.\textsuperscript{155}

Therefore, the Eighth Circuit determined that a typical

\textsuperscript{150} \textit{A Reminder to Hiring Committees}, \textit{supra} note 149.

\textsuperscript{151} \textit{See generally, Gaskell}, 2010 WL 4867630.

\textsuperscript{152} \textit{A Reminder to Hiring Committees}, \textit{supra} note 149

\textsuperscript{153} Wagner, 664 F.3d. at 259, 264.

\textsuperscript{154} \textit{Id.} at 274-75. Teresa Wagner, the plaintiff in this case, was later arrested for drunken driving in 2013. Police say Wagner was arrested when she failed field sobriety tests and a preliminary breath test showed her blood-alcohol content to be above the legal limit. Andrew Altenbaum, \textit{UI Staff member arrested and charged with drunken driving} KWWL.COM (Feb. 13, 2013, 3:22 AM), http://keel.membercenter.worldnow.com/story/21142540/2013/02/13/ui-staff-member-arrested-and-charged-with-drunk-driving.html.

\textsuperscript{155} \textit{Id.} at 270 (quoting Rodriguez-Rios \textit{v.} Cordero, 138 F.3d 22, 24 (1st Cir.1998)).
nondiscrimination test should also apply to cases where discriminatory information is discovered online.\textsuperscript{156} Thus, the First Amendment’s protections of political freedom and speech extend to online information that could easily apply to information discovered during a search with an employee’s or applicant’s password to information available via social media.\textsuperscript{157}

In short, employers are already incentivized not to require social media passwords from applicants or employees because of the possibility of lawsuits.\textsuperscript{158} Even a simple Google or Facebook public search can yield discoverable information that can lead to a claim against the employer if that person is not hired or fired.\textsuperscript{159} Some employers may not heed these warnings, but those employers expose themselves to an applicant’s or employee’s claim, as evidenced by Gaskell and Wagner.\textsuperscript{160} The strategy that an employer uses in the hiring process or review of employees will depend on how much risk the employer is willing to assume. Therefore, legislation would be futile, because employers are already sufficiently disincentivized through the threat of litigation.

\section*{IV. Analysis}

Combining the three primary arguments from above— (1) that the legislation is difficult to enforce; (2) that the laws are preemptively passed; and (3) that an employer should be protecting itself from lawsuits by not asking for any employees’ or job applicants’ passwords for private information that could lead to discrimination or privacy claims— this Note argues that legislative efforts banning employers’ access to passwords are misguided. First, this section explains why legislators should not be passing these acts. Second, the section determines that legislators should, at this time, regulate only within the public sector, rather than overreaching into the private sector, which has not shown a need for regulation regarding online passwords. Overall, because these legislative measures have not been proven to help many people, and because history teaches that

\begin{thebibliography}{9}
\bibitem{156} Id.
\bibitem{157} Id.
\bibitem{158} Id.
\bibitem{159} Hirschfeld & Oliveira, supra note 8.
\bibitem{159} See Wagner, 664 F.3d at 264; Gaskell, 2010 WL 4867630, at *1.
\bibitem{160} See Wagner, 664 F.3d; Gaskell, 2010 WL 4867630.
\end{thebibliography}
government entities would be the primary violators of these laws, the legislators would be better off setting a standard for internal government hiring and firing rather than broadly requiring employers to adhere to a law that is not being broken in the first place.

A. Setting the Stage for Legislative Ineffectiveness

When it comes to the enforcement of these social media acts, many state laws have different enforcement mechanisms, ranging from administrative offenses to criminal offenses. Some other states have no enforcement mechanisms written into their act at all. Thus, enforcement mechanisms and remedies vary from state to state. This hodgepodge of enforcement methods not only makes it confusing for those individuals looking to bring claims against an employer or company but also makes it difficult for attorneys and courts to handle these types of claims and for employers to develop an overall hiring policy.

An individual could either bring a claim in state court or in Federal court under the Password Protection Act. These different opportunities would allow for various remedies for the plaintiff, and assorted penalties for the employer. In turn, these differences would generate confusion for individuals when preparing to bring a claim as to which jurisdiction would be best. Additionally, the differences would allow for preference as to certain courts or jurisdictions for each party, as a state court or Federal court might be more beneficial in terms of a particular remedy or penalty for a given party.

These differences in enforcement mechanisms and penalties also create problems for the legal system overall. Because of the different enforcement provisions, certain jurisdictions are likely to be more favorable to one party than another. Thus, the other party would likely try to remove the case to an alternate, more advantageous jurisdiction. Therefore, the varying enforcement provisions would likely lead to a high number of motions to transfer venue or remove to federal court. That would create a backlog of

---

101 Bernabei & Kabat, supra note 3, at 42.
102 Id.
103 Id.
administrative issues for courts to handle. Because of the increase in time and labor, this backlog would also likely lead to increased attorneys fees for the parties involved.

Enforcement also becomes a problem with respect to what entity would be in charge of regulating the activities of the employers. In one sense, it seems impractical for an existing government department to take on inspection of every company, organization, employer, and school in a certain district. This is especially the case since the U.S. government does not have a regulatory body for privacy invasions of online information and since the DOL has admitted to handling other laws ineffectively.\(^{164}\) Additionally, in this economy, it is simply not reasonable to create a new government body to oversee a new act. Local, state, and federal governments all lack the ability to employ people to act as a watchdog over every company to make sure it does not request disclosure of passwords. A single government entity is not able to police every employer, especially when the overall number of government employees, both at the state and federal levels, is decreasing.\(^{165}\) With a decline in the number of federal inspectors and the lack of any non-governmental agency to fulfill this role, it is ill-advised to require an agency already stretched thin to now review every employment application form in the nation to ensure that the employer is not asking for social media passwords.\(^{166}\) Generally speaking, the funding that is necessary to monitor companies is not available at this time.\(^{167}\)

Without proof that policies invading personal password information affect other applicants or employees, it seems that legislators acted before it was necessary to create a solution to a false problem to please their constituents. If the only occurrences were individuals discussing their stories via the media, the government legislatures have based countless hours of writing and proposing this

\(^{164}\) See Moshell, supra note 96, at 357; U.S. DEPT OF LABOR, DOL ANNUAL REPORT, FISCAL YEAR 2006, PERFORMANCE AND ACCOUNTABILITY REPORT (2006).


\(^{166}\) Thomas, supra note 165.

\(^{167}\) Id.
legislation on a media firestorm. Seemingly, it would have been more efficient for state governments to self-regulate their own policies before assuming most other companies are also requesting passwords. But, with the statistics currently available, there is no evidence to show a need for the password legislation, at least not for the private sector. Thus, it appears that this social media legislation was passed preemptively, without the crucial proof or need for protection.

GINA provides a good example of the problems associated with preemptive legislation.\textsuperscript{168} Since its passage, several complaints over the passage of GINA have arisen.\textsuperscript{169} Without strong statistics to support the reasoning for GINA and its passage, it becomes nearly impossible to measure the act’s effectiveness.\textsuperscript{170} Also, GINA may have legitimized fears regarding discrimination based on genetic information, because it publicized the fear of something that was not fully discussed in the past.\textsuperscript{171} Thus, there arise several issues with preemptive legislation, as exemplified by GINA. Though no real problems have emerged since GINA’s passage, it is not clear whether it has accomplished anything. The time and money spent to pass this law could have been used elsewhere. Thus, like GINA, the laws banning employers’ access to online information are preemptive and raise many of the same concerns. Further, this preemptive passage of such acts may not be the most effective means of preventing problems regarding online discrimination.

Finally, legislators are misusing time and resources in passing these social media laws since it is an employer’s job to protect itself from lawsuits by not asking for passwords or any private information that could lead to liability under discrimination or privacy claims. Employers that review online information, and especially those that gain access to passwords, expose themselves to legal claims ranging from discrimination and Title VII to constitutional privacy and Fourth Amendment issues.\textsuperscript{172}

Oftentimes, for private sector employers, the threat of liability is

\textsuperscript{168} See Roberts, supra note 124 at 484-89.
\textsuperscript{169} See id.
\textsuperscript{170} Id at 489.
\textsuperscript{171} Id.
\textsuperscript{172} See generally Hirschfeld & Oliveira, supra note 9.
more frightening than an unclear and unorganized means of
government enforcement mechanisms employed through the laws
and bills.\textsuperscript{175} A company might rather pay a limited fine or penalty to
the government for its wrongful actions rather than begin a
protracted litigation process, which could involve paying a large sum
to the plaintiff in addition to legal fees and negative publicity.
Therefore, the basic fear of legal actions against an employer
provides a better disincentive to those companies than laws that have
various means of enforcement.

\textit{B. Public Sector Versus Private Sector Legislative Oversight}

Considering the three arguments above, a trend emerges, which
is that the cases involving password requests have stemmed primarily
from local government entities. Because all the prior proof regarding
issues with employers occurred in the public sector, there is no
evidence pointing to a need for protection in the private sector. The
state government positions, and local school districts, have led to the
publicity regarding the requirement to access private online
information. Thus, legislators should be monitoring and regulating
those public sector government agencies and schools, rather than
passing widespread action that affects those without a need for it.

Overreaching legislation can be dangerous. The legal system and
the nature of judicial review are meant to protect against
Congressional overreaching.\textsuperscript{174} Specifically, many people fear that
overreaching legislation takes away the rights of individuals in areas
that have traditionally been protected by the Constitution and the
courts. Since private sector employees already have protections,
government enforcement may not be necessary or even the best,
most efficient means of enforcement, especially if by doing so it
enters a new sphere of government regulation over private
corporations.

Overall, the legislators should be spending their time and
taxpayers’ money in more efficient ways. Whether the proposal and
passage of these social media bills is just a means of enacting
something, or whether the legislators legitimately believe that access

\textsuperscript{175} See Bernabei & Kabat, \textit{supra} note 3, at 42.
\textsuperscript{174} Saikrishna B. Prakash & John C. Yoo, \textit{The Origins of Judicial Review}, 70 U. Chi.
to online information is a formidable problem, these laws are ineffective in their current form. Legislators should have first addressed the problem within the public sector. If online social media access becomes a larger and more widespread occurrence, then that is the time legislators should take action. Additionally, even though the 112th Congress, from 2011-2012, was the least productive Congress on record in the United States passing only near two percent of proposed bills, proposing ineffective and needless bills is not the way to improve productivity or approval ratings. 175

V. CONCLUSION

In the end, the online privacy legislation is ineffective in protecting employees, applicants, and students. The fact that no clear statistics reveal that many people are affected by password requests, in addition to the fact that not many private sector employers are using this practice because of the threat of lawsuits is seemingly enough to show that these laws are not necessary within the private sector. Additionally, the specific proposed laws, and the several that were passed, are preemptive because of the lack of evidence, and also lack effectual enforcement mechanisms.

Rather, these various legislative measures seem to be preemptive in nature, and overreaching in their actions. Overreaching legislation spends unnecessary funds and takes a step beyond what may be allowed. Largely, these acts are not helping many people and are ineffective in their current state. These bills are not a solution to any real problem. Because of the preemptive nature of these acts, there will never be evidence of a bill's actual effect because the problem was nonexistent. Therefore, it is unclear whether there is a need for these bills, and, additionally, whether their enactment creates any effectual or beneficial changes.