5-1-2014

What Are You Looking At? Why the Private Sector's Use of Social Media Need Not Be Legislated

Courteney Brianne Lario

Journal Topic-
Courteney Lario

Title: What Are You Looking At? Why the Private Sector's Use of Social Media Need Not Be Legislated

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 a popular one among legislators, with bills introduced in thirty-six state legislatures and Congress over the past two years aimed at protecting employees or job applicants from employers requesting access to 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 applicants' passwords.[3] The first of these stories involved a governmental entity in Maryland demanding an applicant's Facebook password in 2011.[4] Maryland soon thereafter became the first state to propose and pass a bill, which bans employers from accessing social media passwords and went into effect in October 2012.[5] After several similar stories cropped up across the country, more states began to propose and enact these laws. Currently, six of the thirty-two

---

[1] Press Release, Senator Charles Schumer, Employer Demands for Facebook and Email Passwords as Precondition for Job Interviews may be a Violation of Federal Law; Senators Ask Feds to Investigate (Mar. 26, 2012) (on file at http://www.schumer.senate.gov/Newsroom/record.cfm?id=336396).
[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-passwords-2013.aspx. These numbers are those at the time of publication.
[3] Lynne Bernabei & Alan R. Kabat, *Invasions of Privacy; Congress and state legislatures are properly barring employers' demands for social-media passwords*, 34 NAT'L L.J. 42, 42 (2012).
[4] *Id.*
[5] MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012).

states that have proposed such legislation, California, Delaware, Illinois, Maryland, Michigan, and New Jersey, succeeded in enacting laws in 2012.[6]

Although an increased number of stories have been published regarding employers demanding Facebook passwords, there are questions as to the actual extent of the practice and the necessity for such laws at this time.[7] Several key issues underscore the questionable utility of these laws. First, the laws themselves are difficult to enforce, with no one defined administrative mechanism or specific execution provision. Second, the acts are preemptive and lack substantive facts or figures to warrant their passage. Third, employers already have an incentive 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 later fired or not hired based on social media information, since those 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.[8]

Despite these concerns regarding the recent legislation, state legislatures continue to propose and pass these laws with ease, seemingly as an attempt to help those employees and applicants. Meanwhile, many of the states are themselves the primary entities that have created these online privacy issues in the first place in local government hiring.[9] State legislatures, rather than passing wide-reaching laws that are not necessary, should use their energy to enact

---

[6] National Conference of State Legislatures, Employer Access to Social Media Usernames and Passwords 2012 (2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.
[7] Shel Israel, *The Great Facebook Employee Password Non-Issue*, FORBES (Mar. 25, 2012, 8:32 PM), http://www.forbes.com/sites/shelisrael/2012/03/25/the-great-facebook-employee-password-nonissue/.
[8] Stephen Hirschfeld & Kristin Oliveira, *Keeping Facebook private; States and federal government are introducing legislation to prevent employers from requesting social media passwords*, 136 THE RECORDER 16 (2012).
[9] *See* discussion *infra* Part II.A.

legislation that regulates their own state and local agencies' employment guidelines.[10] Private-sector employers should be permitted to handle matters regarding the hiring and firing process themselves, guided by the legal risks and exposure that come with employment decisions which rely upon candidates' and employees' private online information.[11] Since public and private sector employers have different methods, obligations, and risks associated with employment decisions, legislatures should not over-legislate and lump all employers together in these online privacy acts.[12]

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. This Part reviews the history and reasoning behind the legislative efforts, and dissects the laws themselves. Part II considers three concerns regarding the necessity of these laws. The first is the question of enforceability. The second issue focuses on the lack of evidence justifying these laws in the private sector. The third concern regarding this 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 three primary concerns regarding the necessity of these laws, Part III begins the analysis of how these three issues should affect the

---

[10] T.G. Allison Jr., *Public and Private Management: Are they fundamentally alike in all unimportant respects*, POLICY 1, Vol. 2, 14 (1983).

[11] Anna Hickman, *Don't Bother Asking for Facebook Passwords*, The Corporate Counsel Newsletter, 27 LAW JOURNAL NEWSLETTERS 7, 9 (Aug. 16, 2012).

[12] Joe Weisenthal, *The Public Sector vs. The Private Sector in One Colossal Chart*, http://www.businessinsider.com/chart-the-public-vs-private-sector-2012-7; Allison Jr., *supra* note 10, 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, at 21-22.

passage of the legislation. Finally, this Note concludes that state and federal legislatures, rather than addressing the wide-spectrum of both public and private sector employers, should limit such legislation to only the public sector. There is yet to be a need for laws regarding online privacy information beyond the public sector where, as here, the other concerns of enforceability and means of protection for any injured employee or applicant outweigh the need for private sector regulation.

Part I: Background

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

A. History

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 legislatives measures. The first major issue occurred in Maryland in 2011[13] When the Maryland Department of Public Safety and Correctional Services required the Facebook password of a corrections officer in his recertification process, supposedly attempting to determine whether the officer had ties to gang members.[14] The American Civil Liberties Union ("ACLU") of Maryland took a stance against this new practice in a press release issued in

[13] Bernabei & Kabat, *supra* note 3, at 42.
[14] *Id.*

February 2011.[15] The ACLU also posted a YouTube video highlighting the story and requesting that the Department no longer request online passwords.[16] In response, the Department did suspend the practice.[17] Nevertheless, soon thereafter in May 2012, Governor Martin O'Malley of Maryland signed into law the online privacy act, proposed and passed by the Maryland legislature.[18] This law was the first of its kind and marked the beginning of a nationwide trend.[19]

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.[20] In June of 2009, the city manager of Bozeman issued a statement suspending the city's requirement but only after the city government received many complaints from its citizens about this practice.[21] On February 27, 2013, Montana's state Senate passed a bill protecting private electronic information of job applicants and employees.[22] The bill currently awaits a vote in the state House of Representatives.[23]

A third issue arose in Minnesota, when a young girl came forward saying that her public school demanded she provide her login information to Facebook and email accounts.[24] The girl said that the school asked for her passwords because of allegations that she was having

---

[15] Press Release, The American Civil Liberties Union of Maryland, Want a Job? Password Please! (Feb. 14, 2011) (on file at http://www.aclu-md.org/press_room/40).
[16] Aaron C. Davis, *Maryland corrections department suspends Facebook policy for prospective hires*, WASH. POST., Feb. 22, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207486.html.
[17] *Id.*
[18] MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012).
[19] National Conference of State Legislatures, Employer Access to Social Media Usernames and Passwords 2012 (2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.
[20] Declan McCullagh, *Want a job? Give Bozeman your Facebook, Google Passwords*, CNET, June 18, 2009, http://news.cnet.com/8301-13578_3-10268282-38.html.
[21] *Id*; David Pardo, *Bozeman, Montana Suspends Controversial Requirement that Job Applicants Provide Usernames and Passwords to Facebook Accounts*, SECURITY, PRIVACY AND THE LAW, July 15, 2009, *available at* http://www.securityprivacyandthelaw.com/2009/07/bozeman-montana-suspends-controversial-requirement-that-job-applicants-provide-usernames-and-passwords-to-facebook-accounts/.
[22] S.B. 195, 63d Leg. (Mont. 2013).
[23] *Id*; 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-passwords.aspx.
[24] Press Release, American Civil Liberties Union of Minnesota, ACLU-MN Files Lawsuit Against Minnewaska Area Schools (Mar. 6, 2012) (on file at http://www.aclu-mn.org/news/2012/03/06/aclu-mn-files-lawsuit-against-minnewaska-area-schools).

conversations about sex with another student.[25] Supposedly, the school administrator informed the girl that she would be punished if she did not provide the information.[26] The ACLU of Minnesota filed a lawsuit in 2012 against the girl's school district,[27] the Minnewaska Area Schools, as well as the Pope County Sheriff's office for violating the constitutional rights of a minor student, specifically arguing 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.[28]

Besides these issues that arose from state or local government actions, there has also been a general trend in the federal government requiring more detailed and in-depth information for job applicants.[29] President Barack Obama created a more comprehensive vetting process for high-ranking executive branch applicants than previous, including requiring disclosure of any "e-mail(s) that might embarrass the president-elect, along with any blog posts and links to their Facebook pages."[30] Although the executive branch application did not require applicants to relay their username or passwords for social media websites, it did require information regarding

---

[25] *Id.*
[26] *Id.*
[27] 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. v. Minnewaska Area School District, Civ. No. 12-588, 2012 WL 3870868, at *1 (D. Minn.Sept. 6, 2012).
[28] *Id*; Complaint at 2, R.S. v. Minnewaska Area School District. (No. 12-588), 2012 WL 3870868, at *1 (D. Minn.Sept. 6, 2012).
[29] *See generally* Jackie Calmes, *For a Washington Job, Be Prepared to Tell All*, N.Y. TIMES, Nov. 12, 2008, *available at* http://www.nytimes.com/2008/11/13/us/politics/13apply.html?_r=2&. (discussing President Barack Obama's seven-page questionnaire, which included 63 requests for personal and professional records, for high-ranking applicants for the President's first administration).
[30] *Id.*

private Internet posts or e-mails.[31] Thus, the federal government created a standard of all-encompassing application inquiries, covering information from new forms of online data.[32]

Each of these controversies arose out of requirements for information from a governmental entity.[33] 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.[34] Despite the trend toward government transparency, these acts raise some questions as to whether these requests are going too far.[35] Thus, in reaction to these issues, specifically after the Maryland story came out, state legislatures decided it was time to take action.[36]

B. Legislative Overview

As of the writing of this article, thirty-six state legislatures have now proposed or passed legislation banning access to social media passwords.[37] Congress has also proposed legislation of this kind.[38] 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.[39] Eight other states proposed online

---

[31] *Id.*
[32] *Id.*
[33] *See id. at* 4-5.
[34] McCullagh, *supra* note 20.
[35] Calmes, *supra* note 29.
[36] National Conference of State Legislatures, Employer Access to Social Media Usernames and Passwords 2012 (2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.
[37] *Id.*
[38] Password Protection Act of 2012, H.R. 5684, 112th Cong. (2nd Sess. 2012); Social Networking Online Protection Act, H.R. 537, 112th Cong. (2nd Sess. 2012).
[39] CAL. LAB. CODE § 980 (West 2012); DEL. CODE ANN. TIT. 14, §§ 9401-9405 (West 2012); 820 ILL. COMP. STAT. 55/10 (2012); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); MICH. COMP. LAWS §§ 37.271-37.278 (2012); N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012); New Jersey's state legislature passed the legislation unanimously in

privacy legislation in 2012: Massachusetts, Minnesota, Missouri, New York, Ohio, Pennsylvania, South Carolina, and Washington.[40] Utah is the only state, thus far, to pass its act in 2013.[41] An additional twenty-one states proposed laws in 2013: Arizona, Arkansas, Colorado, Connecticut, Georgia, Hawaii, Iowa, Kansas, Maine, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Oregon, Rhode Island, Texas, Vermont, and West Virginia.[42]

Two separate acts were proposed in Congress in April 2012: H.R. 5684, the Password Protection Act of 2012, and H.R. 5050, the Social Networking Online Protection Act.[43] The Password Protection Act would prohibit employers from requiring job applicants and employees to provide access to their private online accounts.[44] This act would apply to employers' use of any online password information as a condition of employment, discrimination, or retaliation.[45] 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."[46] The Social Networking Online Protection Act, alternatively, would prohibit employers and schools from requiring or requesting that employees,

---

October, 2012. Martin Bricketto, *NJ Senate Oks Bill Shielding Workers' Social Media Privacy*, LAW360, Oct. 25, 2012, http://www.law360.com/articles/389441/nj-senate-oks-bill-shielding-workers-social-media-privacy.

[40] H.D. 4323, (Mass. 2012); H.F. 2982, 87th Leg., (Minn. 2012); H.B. 2060, 97th Leg., 1st Reg. Sess. (Mo. 2012); S.B. 6938, 235th Leg. (N.Y. 2012); S.B. 351, 129th Leg. (Ohio 2012); H.B. 2332 (Pa. 2012); H.B. 1505, 119th Leg. (S.C. 2012); S.B. 6637, 62nd Leg., 1st Spec. Sess. (Wash. 2012).

[41] UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).

[42] S.B. 1411, 51st Leg., 1st Reg. Sess. (Ariz. 2013); H.B. 1901 & 1902, 89th Leg., Reg. Sess. (Ark. 2013); H.B. 1046, 69th Leg., 1st Reg. Sess. (Colo. 2013); H.B. 5690 (Conn. 2013); H.B. 149 (Ga. 2013); H.B. 713, 27th Leg., Reg. Sess. (Haw. 2013); H.F. 272 (Iowa 2013); H.B. 2094 (Kan. 2013); H.B. 838, 126th Leg., 1st Reg. Sess. (Me. 2013); H.B. 165, 56th Leg., Reg. Sess. (Miss. 2013); S.B. 195, 63d Leg. (Mont. 2013); L.B. 58, 103rd Leg., 1st Sess. (Neb. 2013); A.B. 181, 77th Leg., Reg. Sess. (Nev. 2013); H.B. 414 (N.H. 2013); S.B. 371, 51st Leg., 1st Sess. (N.M. 2013); H.B. 1455, 63rd Leg., Reg. Sess. (N.D. 2013); S.B. 499, 77th Leg., Reg. Sess. (Or. 2013); S.B. 493 (R.I. 2013); S.B. 416, 83rd Leg., Reg. Sess. (Tex. 2013); S.B. 7 (Vt. 2013); H.B. 2966, 81st Leg., 1st Sess. (W. Va. 2013).

[43] H.R. 5684; H.R. 537.

[44] H.R. 5684; Hirschfeld & Oliveira, *supra* note 8.

[45] H.R.5684.

[46] Bernabei & Kabat, *supra* note 3, at 42(quoting Lewis and Roca LLP, *The Computer Fraud and Abuse Act: 'Authorization' in Flux and the Ninth Circuit Dilemma*, Mar. 6, 2012, http://www.jdsupra.com/post/documentViewer.aspx?fid=75d0f53e-e6ce-4165-a5dd-6fcd64a98470).

students, and job applicants provide a username or password to access a personal account on any social networking website.[47] 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.[48]

C. Enforcement Techniques

Of the seven states that have passed legislation banning access to online information, six now ban both employers and schools from "requesting or requiring" any usernames or passwords to online information.[49] Delaware passed an act that banned only academic institutions from requiring online password information.[50]

Of these seven laws, only three of them have specified means of enforcing an employer's or school's actions.[51] Utah's Internet Privacy Amendments 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.[52] 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.[53] However, Michigan's Act also provides that a person who violates this Act is guilty of a misdemeanor.[54] Therefore, Michigan's Act takes a step further than Utah's and makes a violation a criminal action.[55]

---

[47] H.R. 537; Hirschfeld & Oliveira, *supra* note 8.
[48] *Id.*
[49] CAL. LAB. CODE § 980 (West 2012); DEL. CODE ANN. TIT. 14, §§ 9401-9405 (West 2012); 820 ILL. COMP. STAT. 55/10 (2012); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); MICH. COMP. LAWS §§ 37.271-37.278 (2012); N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012); UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).
[50] DEL. CODE ANN. TIT. 14, §§ 9401-9405 (West 2012)
[51] CAL. LAB. CODE § 980 (West 2012); DEL. CODE ANN. TIT. 14, §§ 9401-9405 (West 2012); 820 ILL. COMP. STAT. 55/10 (2012); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); MICH. COMP. LAWS §§ 37.271-37.278 (2012); N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012); UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).
[52] UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).
[53] MICH. COMP. LAWS §§ 37.271-37.278 (2012).
[54] *Id.*
[55] *Compare* MICH. COMP. LAWS §§ 37.271-37.278 (2012), *with* UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).

The only other state law that includes a specific violation and enforcement provision is New Jersey's, which again provides that an aggrieved individual may institute a civil action.[56] Unlike Utah's and Michigan's Acts, 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.[57]

Thus, overall among the seven state laws that ban some sort of access to online passwords, four state laws have no specific enforcement provision, three allow for civil actions, two specify an upper limit for any award of damages, and one imposes criminal sanctions.[58]

When it comes to enforcement provisions of the federal bills, both bills include more stringent and severe violation penalties.[59] Since the Password Protection Act would be interwoven with the Computer Fraud and Abuse Act, enforcement provisions already exist.[60] 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.[61] The Social Networking Online Protection Act, on the other hand, is very clear that its remedy is a civil violation is actionable by the Secretary of Labor.[62] Additionally, an employer that violates the Social Networking Online Protection Act can pay a fine of no more than $10,000.[63] Therefore, the two

---

[56] N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012).
[57] *Compare* N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012), *with* MICH. COMP. LAWS §§ 37.271-37.278 (2012), *and* UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).
[58] CAL. LAB. CODE § 980 (West 2012); DEL. CODE ANN. TIT. 14, §§ 9401-9405 (West 2012); 820 ILL. COMP. STAT. 55/10 (2012); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); MICH. COMP. LAWS §§ 37.271-37.278 (2012); N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012); UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).
[59] H.R. 5684; H.R. 537.
[60] Computer Fraud & Abuse Act, 18 U.S.C. § 1030 (1986).
[61] *Id.*
[62] H.R. 537.
[63] *Id.*

federal acts include provisions for harsher penalties and would allow for stricter enforcement via civil suit and the Secretary of Labor.[64]

D. Goals Behind Legislation

Each of the proposed bills or enacted statutes provides some restrictions against employers requesting employees' or applicants' online passwords.[65]

> This 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.[66]

Generally, employers are not able to gain non-workspace information without the employee's consent.[67] The legislators do not seem to be convinced by entities' explanations 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 resume fraud.[68] Where the bills have been successful the state legislatures view gaining access to social media passwords as an invasion of an individual's privacy and as a result seek to protect employees from these requests, in addition to providing a remedy in case the law is not followed.[69]

Part II: 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,

---

[64] H.R. 5684; H.R. 537.
[65] Bernabei & Kabat, *supra* note 3, at 42.
[66] *Id.*
[67] *Id.*
[68] Hirschfeld & Oliveira, *supra* note 8.
[69] *See generally id.* (parenthetical).

there is no clear proof of how many employers or government bodies are requesting these passwords, and not enough studies or statistics to glean the number of applicants affected by these password requests. Therefore, these legislatures are preemptively passing acts without proof of their actual necessity. 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.

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.[70] There are several reasons why this legislation is difficult to enforce: (1) varying enforcement mechanisms 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 government's enforcement power over the employer outside the public-sector is uncertain.[71]

A major problem with enforcement is that many of the current bills have differing enforcement mechanisms or are lacking them altogether.[72] Bills from different states provide assorted enforcement actions, as discussed above.[73] While some states, such as New Jersey and Utah provide private civil rights of action, other states, such as Michigan, create a misdemeanor

[70] Bernabei & Kabat, *supra* note 3, at 42.
[71] *See* discussion *infra* Part II.A.
[72] *See* discussion *supra* Part I.C.
[73] *Id.*

offense in addition to the civil and administrative remedies.[74] Additionally, Utah and Michigan provide limited damages that a court can award to an aggrieved claimant, while New Jersey sets no specific damage limit.[75] On the other hand, the bills proposed in other states, such as California, Maryland, Missouri, and South Carolina provide no enforcement mechanism whatsoever.[76] 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.[77] In that case, a full range of remedies would presumably be available.[78] These varying enforcement measures make it difficult for national employers to create and defend regulations for the company as a whole. In Michigan, the company may be up for criminal charges, while in Utah the company only has to pay a fine of $500.[79]

The congressional bills would also be difficult to enforce.[80] Specifically, the Social Networking Online Protection Act "allows for enforcement only through the U.S. DOL, at a time when that agency lacks the resources to enforce other federal employment statutes."[81] 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 causes of action.[82] This confusion again leads to difficulty for large national companies that span several or all states, for that company could get sued by an individual in one state and pay a

---

[74] *Compare* N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012), *and* MICH. COMP. LAWS §§ 37.271-37.278 (2012), *with* UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).
[75] *Compare* UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012), *and* MICH. COMP. LAWS §§ 37.271-37.278 (2012), *with* N.J. STAT. ANN. §§ 18A:3-29- 18A:3-32 (2012).
[76] CAL. LAB. CODE § 980 (West 2012); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); H.B. 2060, 97th Leg., 1st Reg. Sess. (Mo. 2012); H.B. 1505, 119th Leg. (S.C. 2012).
[77] Bernabei & Kabat, *supra* note 3, at 42.
[78] *Id.*
[79] MICH. COMP. LAWS §§ 37.271-37.278 (2012); UTAH CODE ANN. §§ 34-48-101- 34-48-301 & 53B-24-101- 53B-24-301 (2012).
[80] H.R. 5684; H.R. 537.
[81] 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, 1176-77 (1983).
[82] H.R. 537

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.[83] However, 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.[84]

Another reason enforcement is impractical is because, where private suit is not authorized, it is nearly impossible for the government to regulate, watch, and monitor every employer in a certain jurisdiction. First, the United States has embraced an ideal that the Internet should primarily be self-regulated.[85] Thus, the U.S. does not have a regulatory body for invasions of privacy when it comes to online information.[86] Additionally, the Department of Labor ("DOL"), a department that could regulate this act federally, already "administers and enforces more than 180 federal laws."[87] In a 2006 Performance and Accountability Report ("PAR"), the DOL assessed twenty-eight of its programs to determine each programs' effectiveness.[88] Out of the twenty-eight programs reviewed under the PAR, one was rated "effective," eight were rated "moderately effective," twelve were deemed "adequate," and the last four were ranked

---

[83] H.R. 5684.
[84] *Id.*
[85] Privacy Int'l, Privacy and Human Rights 2003: Overview, http://www.privacyinternational.org/survey/phr2003/overview.htm (last visited Oct. 29, 2004); *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 TX. TECH. L. REV. 357 (2005) (discussing how the United States should develop a more comprehensive data-protection regime).
[86] *See generally id.*
[87] U.S. DEPARTMENT OF LABOR, Summary of the Major Laws of the Department of Labor, *available at* http://www.dol.gov/opa/aboutdol/lawsprog.htm. (GLOBAL: for these executive materials, see Rule 14 pg. 135. You can small-caps the Department name as well as the title, and then add the date).
[88] U.S. DEPARTMENT OF LABOR, DOL Annual Report, Fiscal Year 2006, Performance and Accountability Report (2006).

"ineffective."[89] The DOL has also specifically admitted to ineffectively enforcing certain acts in the past.[90]

A third major issue with enforcement is funding.[91] In this economic circumstances that the United States now faces, the government is looking for measures to cut spending.[92] "There surely are more economic shocks in store, including increased unemployment, more corporate defaults, and state and local government budget emergencies."[93] In creating jobs or a government entity to oversee employers in regard to this new legislation, only a further buildup of resources and funding would occur in the public sector. But over the past year local, state, and federal government jobs have dropped by 162,800 jobs, a .7 percent decline.[94] With declining job numbers in the government sector, and the goal to cut government spending, including a recent sequester, there is no money or manpower left to create an entity or pay more employees to monitor employers and their online information usage.[95]

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 legislations, the infeasibility of enforcement, the lack of funds needed to enforce these laws, and the question as

---

[89] *Id.*
[90] Kopelman, *supra* note 82, at 1176-77.
[91] *See generally* RICHARD A. POSNER, A FAILURE OF CAPITALISM: THE CRISIS OF '08 AND THE DESCENT INTO DEPRESSION (Harvard Univ. Press, 2009).
[92] *See* Eamon K. Moran, Wall Street Meets Main Street: Understanding the Financial Crisis, 13 N.C. BANKING INST. 5 (2009).
[93] *Id.* at 10.
[94] G. Scott Thomas, *Government employment drops by 162,800 jobs*, THE BUSINESS JOURNALS (Aug. 17, 2012), http://www.bizjournals.com/bizjournals/on-numbers/scott-thomas/2012/08/government-employment-drops-by-162800.html.
[95] *Id.*

to whether it should be the government's responsibility to monitor these employers lead to the impracticability of implementing these laws, both administratively and functionally.[96]

B. Preemptive Legislation

Many of the controversies surrounding the password requests occur in state government entities.[97] But, rather than the states handling these issues with state government policies, specifically hiring policies, the states decided to legislate against these practices in both the public and private sectors.[98] Beyond these state or local government accounts, there is reason to doubt that many companies, employers, or schools are requesting online passwords.[99] Shel Israel, of Forbes states that

> There 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.[100]

In his article, Israel argues that these online privacy bills are proposed without any proof as to how many people are affected.[101] Specifically, he states that this is a non-issue that has been turned into a large concern.[102]

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

---

[96] *See* discussion *supra,* Part II. A.
[97] *See* Bernabei & Kabat, *supra* note 3; *see also,* discussion *supra* P. II, 3-6.
[98] Bernabei & Kabat, *supra* note 3.
[99] Israel, *supra* note 7.
[100] *Id.*
[101] *Id.*
[102] *Id.*

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.[103] The "recent reports" that the press release makes reference to are three media stories to individual narratives.[104]

> 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.[105]

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.[106]

In fact, when it comes to available statistics regarding how many employers are requiring an online password, there are not many studies in existence. In one poll, however, of over 1,000 high-level companies completed by Littler Mendelson, P.C., fewer than one percent of those companies said that they had "requested social media logins as part of the hiring or onboarding process."[107] Though this does not cover all companies, it strongly suggests that almost none of the most successful private sector entities are requesting social media passwords.[108]

---

[103] *See* Press Release, Senator Charles Schumer, *supra* note 1.
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] Littler Mendelson Executive Employer Survey Report15 (June 2012), http://shared.littler.com/tikit/2012/12_EE_survey_communication/Littler_Mendelson_Executive_Employer_Survey_Report_2012.pdf. Out of the 1,000 high-level companies, the respondents were comprised of seven percent C-suite executives, 45 percent in-house attorneys, 41 percent human resources professionals, and seven percent other professionals. *Id.* at 17. Additionally the sizes of the companies were comprised of 21 percent LargeCap, or greater than four billion dollars in market capitalization; 21 percent MidCap, or one to four billion in market capitalization; 36 percent SmallCap, or less than one billion in market capitalization, and 22 percent did not respond with particular size. *Id.*
[108] *Id.*

This is not the first time, however, that legislation has been enacted to deal with a supposed problem without statistics and evidence to document the existence of the problem in the first place. .[109] A recent act passed preemptively was the Genetic Information Nondiscrimination Act ("GINA"), [110] which was passed by Congress in 2008 to prohibit employers from discriminating against employees or applicants based on genetic information.[111] 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.[112] 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.[113] Therefore, Congress seemed to preemptively pass GINA without solid statistics or any strong evidence for its need.[114]

Though GINA protects against possible discrimination based on genetic information, there are some downsides of GINA having been preemptively passed.[115] One negative is it is nearly impossible to measure the Act's effectiveness without prior statistics.[116] Therefore, discovering whether the legislation has actually protected anyone is nearly impossible.[117] Another consequence of Congress passing GINA preemptively is that GINA "may fail to

---

[109] Jessica Roberts, *Preempting Discrimination: Lessons from the Genetic Information Nondiscrimination Act*, 63 VAND. L. REV. 439, 465-66 (2010), *available at* http://www.vanderbiltlawreview.org/articles/2010/03/Roberts-Preempting-Discrimination-63-Vand.-L.-Rev.-439-2010.pdf.
[110] *Id.*
[111] The Genetic Information Nondiscrimination Act of 2008, Information for Researchers and Health Care Professionals, HHS (Apr. 6, 2009), *available at* http://www.genome.gov/Pages/PolicyEthics/GeneticDiscrimination/GINAInfoDoc.pdf.
[112] *Genetic Information Nondiscrimination Act of 2008: Hearing on H.R. 493 Before the H* (include specific house committee)., 110th Cong. Page # if applicable (2007) (introductory remarks by Hon. Louise M. Slaughter of New York).
[113] Roberts, *supra* note 115, at 465-66.
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*

alleviate (or may even legitimize) fears of genetic-information discrimination."[118] Because Congress passed GINA before genetic discrimination affected many people, it seems possible that GINA raises more awareness about genetic discrimination than is desirable,[119] Including generating fears of discrimination that did not previously exist.[120] Rather than protecting and assuaging peoples' fears, it creates and stimulates the necessity of that fear.[121]

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.[122] Without much data, therefore, the password legislation seems also to be preemptive, and thus encounters those same problems that GINA does. Typically, and in the past, discriminatory legislation was passed retroactively.[123]

C. Employers' Disincentives

Employers open themselves up to lawsuits by looking into online information, specifically by viewing private personal information.[124] 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,.[125] If an applicant is not hired after providing social media access, that applicant can later claim that said information was the reason.[126] These employers, who review online information or require social media passwords, open themselves up to claims ranging from discrimination and retaliation to constitutional or

---

[118] *Id.*
[119] *See id.*
[120] Roberts, *supra* note 115, at 465-66.
[121] *Id.* at 490.
[122] *Id.*
[123] *Id.* at 457.
[124] Hickman, *supra* note 11, at 9.
[125] Hirschfeld & Oliveira, *supra* note 8.
[126] *Id.*

tort-based privacy issues.[127] For example, Title VII states that it is unlawful for an employer to discriminate based on race, color, religion, sex, or national origin.[128] The First Amendment also protects freedom of speech; and freedom of religion.[129] 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.[130]

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.[131] While the 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.[132]

Gaskell v. University of Kentucky, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010), involves a discrimination claim under Title VII.[133] Gaskell alleged the university rejected him after the hiring committee found information on his religious views during an Internet search.[134] Though this case does not involve requesting online passwords, it shows that even a basic Internet search opened the employer to liability based on the information discovered.[135] 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.[136] Although this case settled, it reveals that a triable issue of

---

[127] *See generally, id.*
[128] 42 U.S.C.A. § 2000e-2.
[129] USCA CONST Amend. I.
[130] Restatement (Second) of Torts § 652B (1977).
[131] *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); *see also* Alvarez & Ruff, *supra* note 99.
[132] *See* Wagner v. Jones, 664 F.3d 259 (8th Cir. 2011); Gaskell v. Univ. of Kentucky, 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010); *see also* Alvarez & Ruff, *supra* note 99.
[133] *See* Gaskell, 2010 WL 4867630.
[134] Gaskell, 2010 WL 4867630, at *3.
[135] *See generally, id.*
[136] *Id.* at *1; *A Reminder to Hiring Committees: Don't Google the Candidates?*, PrawsBlawg (Aug. 29, 2012), http://prawfsblawg.blogs.com/prawfsblawg/getting_a_job_on_the_law_teaching_market/.

fact can exist in a discrimination claim from discovered online information.[137] Therefore, 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.[138]

A second example is *Wagner v. Jones*, 664 F.3d 259 (8th Cir. 2011),[139] which involved the University of Iowa's College of Law and its failure to hire a writing instructor, whose political beliefs were available online.[140] In the end, the court found that Wagner[141], the applicant, had presented enough evidence of discrimination that the case could be brought to a jury.[142] On appeal, the Eighth Circuit applied the following test:

> 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.[143]

Therefore, the Eighth Circuit determined that a typical nondiscrimination test should also apply for cases in which discriminatory information is discovered through online means.[144] And thus, the First Amendment with its political freedom and freedom of speech provisions applies to

---

[137] *A Reminder to Hiring Committees: Don't Google the Candidates?*, PrawsBlawg (Aug. 29, 2012), http://prawfsblawg.blogs.com/prawfsblawg/getting_a_job_on_the_law_teaching_market/.
[138] *Id.*
[139] *See Wagner*, 664 F.3d. at 264.
[140] *Id.* at 264.
[141] 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. CBS 2 IOWA, February 13, 2013, http://www.cbs2iowa.com/shared/newsroom/top_stories/videos/kgan_vid_14208.shtml.
[142] *Id.* at 274-75.
[143] *Id.* at 270 (quoting Rodriguez–Rios v. Cordero, 138 F.3d 22, 24 (1st Cir.1998).
[144] *Id.*

online information, and could also apply to information discovered during a search with an employee's or applicant's password to information available via social media.[145]

In short, employers are already incentivized not to require passwords from applicants or employees because of the possibility of lawsuits.[146] 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.[147] Some employers may not heed these warnings. However, those employers expose themselves to an applicant's or employee's claim, as evidenced by *Gaskell* and *Wagner*.[148] The strategy that the employer uses in the hiring process or when reviewing employees will depend on how much risk the employer is willing to assume.

Part III: 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 any private information that could lead to discrimination or privacy claims—this Note argues that legislative efforts banning access to employers' access to passwords is mistaken. 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 government entities would be the primary violators of these laws, the legislators would be better off setting a standard for internal government hiring

---

[145] *Id.*
[146] Hirschfeld & Oliveira, *supra* note 8.
[147] *See Wagner,* 664 F.3d at 264; Gaskell, insert year WL 4867630, at *1; *see also* Alvarez & Ruff, *supra* note 99.
[148] *See Wagner*, 664 F.3d; Gaskell, WL 4867630.

and firing rather than broadly requiring employers to adhere to a law that most are not breaking in the first place.

A. Setting the Stage for Legislative Ineffectiveness

When it comes to the enforcement of the acts, many state laws have different enforcement mechanisms, ranging from administrative enforcement to criminal offenses.[149] Some other states have no enforcement written into the act at all.[150] Thus, enforcement mechanisms and remedies vary state to state. This hodgepodge of enforcement methods not only make it confusing for those individuals looking to bring claims against an employer or company, but also make it difficult for attorneys and courts to handle these types of claims.

An individual could either bring a claim in state courts or federally under the Password Protection Act. These different opportunities could allow for various remedies for the plaintiff, and assorted penalties for the employer.[151] 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 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 and remove the case to an alternate, more advantageous district. 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 administrative issues for courts to handle. Because of the

[149] Bernabei & Kabat, *supra* note 3, at 42.
[150] *Id.*
[151] *Id.*

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.[152] 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. Additionally, in this economy, it is simply not reasonable for a single entity to police an employer, especially when the overall number of government employees, both at the state and federal levels, is decreasing.[153] 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 yet still charged with enforcing hundreds of federal laws and regulations as well as the oversight of every federal employment law, to now review every employment application form in the nation to ensure that the employer is not asking for social media passwords in order to quell a problem for which there is no empirical

---

[152] *See* Ryan Moshell, *...And then there was one: The outlook for a self-regulatory United States amidst a global trend toward comprehensive data protection*, 37 TX. TECH. L. REV. 357 (2005); U.S. DEPARTMENT OF LABOR, DOL Annual Report, Fiscal Year 2006, Performance and Accountability Report (2006).

[153] G. Scott Thomas, Government employment drops by 162,800 jobs, THE BUSINESS JOURNALS (Aug. 17, 2012), http://www.bizjournals.com/bizjournals/on-numbers/scott-thomas/2012/08/government-employment-drops-by-162800.html; *See generally*, RICHARD A. POSNER, A FAILURE OF CAPITALISM: THE CRISIS OF'08 AND THE DESCENT INTO DEPRESSION, (Harvard Univ. Press 2009).

evidence to show that it even exists.[154] Generally speaking, the funding that is necessary to monitor companies is not available at this time.[155]

Without proof that other applicants or employees have been affected by policies invading personal password information, 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 legislation on media firestorm. Seemingly, it would have been much easier, faster, and simpler for the state governments to self-regulate their own policies before assuming most other companies are also requesting passwords. But, with the statistics currently available, evidence showing a need for the password legislation does not present itself, 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.

A good example of the problem of preemptive legislative action is GINA.[156] Since its passage, several complaints over the passage of GINA have arisen.[157] Without strong statistics to support the reasoning for GINA and its passage, it becomes nearly impossible to measure the effectiveness of the acts.[158] Also, GINA may also have legitimized fears regarding discrimination based on genetic information, because it publicized the fear of something that was not much discussed previously.[159] 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

---

[154] *Id.*
[155] *See id.*
[156] *See generally* Roberts, *supra* note 115.
[157] *See id.*
[158] *Id.*
[159] *Id.*

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 because an employer should be protecting itself from lawsuits by not asking for any employee's or job applicant's passwords for any private information that could lead to discrimination or privacy claims. Employers that review online information, and especially those that gain access to private passwords, expose themselves to legal claims ranging from discrimination and Title VII to constitutional privacy and Fourth Amendment issues.[160]

Often times, for private sector employers, the threat of liability is more frightening than an unclear and unorganized means of enforcement mechanisms employed through the laws and bills.[161] 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. 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.

B. Public Sector v. Private Sector Legislative Oversight

Considering the three arguments from above, a trend emerges. That trend 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,

[160] *See generally* Hirschfeld & Oliveira, *supra* note 8.
[161] Bernabei & Kabat, *supra* note 3, at 42.

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.[162] 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. And, since private sector employees already have protections, the government may not be necessary or 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 the taxpayers' money in more efficient ways. 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.[163] 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 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.

Conclusion

---

[162] Saikrishna B. Prakash & John C. Yoo, *The Origins of Judicial Review*, 70 U. CHI. L. REV. small caps 887, page # n. 20 (2003).

[163] Stephen Dinan, *Capitol Hill least productive Congress ever: 112th fought 'about everything'*, THE WASHINGTON TIMES, January 9, 2013, http://www.washingtontimes.com/news/2013/jan/9/capitol-hill-least-productive-congress-ever-112th-/?page=all; Susan Davis, *This Congress could be least productive since 1947*, USA TODAY, Aug. 15, 2012, http://usatoday30.usatoday.com/news/washington/story/2012-08-14/unproductive-congress-not-passingbills/57060096/1.

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. This bill is not a solution to any real problem. And though it is seemingly preemptive, there will never be evidence of its actual effect because the problem was nonexistent.