PASSWORD PROTECTION NOW: AN ELABORATION ON THE NEED FOR FEDERAL PASSWORD PROTECTION LEGISLATION AND SUGGESTIONS ON HOW TO DRAFT IT♦

INTRODUCTION

On March 26, 2012, Senators Charles Schumer (D-NY) and Richard Blumenthal (D-CT) sent letters to the Department of Justice and the Equal Employment Opportunity Commission urging them to launch a federal investigation into the legality of asking job applicants to divulge their usernames and passwords for social networking and email websites as a prerequisite to hiring.[1] The letters were prompted by reports indicating that employers across the country were demanding private information from job applicants as part of the interview process, including photos and personal messages not shared with anyone else.[2] Social media provide useful platforms for job applicants and employers to interact, but they also frequently serve as the vehicles through which employers discover unfavorable material that proves fatal to employment prospects.[3] The current trend toward using social

[1] Press Release, Senator Charles E. Schumer, Blumenthal, 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), http://www.schumer.senate.gov/Newsroom/record.cfm?id=336396.

[2] *Id. See* Michelle Singletary, *Would You Give Potential Employers Your Facebook Password?*, WASH. POST, Mar. 29, 2012, http://www.washingtonpost.com/business/economy/would-you-give-potential-employers-your-facebook-password/2012/03/29/gIQAlJiqiS_story.html.

[3] Bob Sullivan, *Social Networking Can Doom Job Prospects*, RED TAPE CHRONICLES ON MSNBC (Sept. 30, 2011), http://donsdocs.files.wordpress.com/2011/12/social-networking-can-

networking websites as a primary vehicle for effecting positive social and political change establishes social networking sites as the digital age's "public square" for important discourse.[4] By enacting password protection legislation, states have signaled concern that permitting employers and academic institutions to demand employees, students, and applicants to provide access to their social media accounts could substantially chill the discourse that occurs on social networking websites.[5]

The prevalence and accessibility of social media have made online background checks on prospective employees common practice.[6] By directly accessing password-protected social media, employers may view information that is not visible to the online "public"; indeed, they are able to browse through users' password-encrypted accounts as though they are authorized users and privy to intimate photographs, communications, and other sensitive information. Similar screening procedures include "shoulder surfing," accessing social media applications without entering a password through personal communications devices such as smartphones and tablets, and requiring that applicants accept a "Friend Request" from a company representative.[7] Orin Kerr, a George Washington University law professor and former federal prosecutor, commented that these invasive screening procedures constitute "an egregious privacy violation"; he

doom-job-prospects.pdf.

[4] H.R. 308, 146th Gen. Assemb. (Del. 2012); Education Privacy Act, H.R. 309, 146th Gen. Assemb. (Del. 2012).

[5] *Supra*, note 4.

[6] A survey commissioned by CareerBuilder.com in 2007 found that nearly half of employers (45%) use the Internet for screening applicants. Mike Maciag, *As Potential Employers Begin to Poke Around in Facebook and Myspace . . . Personal Sites May Not Be Your Friend*, PEORIA JOURNAL STAR, Mar. 4, 2008, *available at* http://iw.newsbank.com/iw-search/we/InfoWeb?p_action=doc&p_theme=aggdocs&p_topdoc=1&p_docnum=1&p_sort=YMD_date:D&p_product=AWNB&p_docid=11FF37AF3B492B78&p_text_direct-0=document_id=(%2011FF37AF3B492B78%20)&p_multi=PJSB&s_lang=en-US&p_nbid=Y6BQ55WRMTM2NDI0Nzk3NS4xMzAyOTM6MTo4OnBlb3JpYXBs. "In 2006, a similar CareerBuilder.com survey found 63 percent of the hiring managers that viewed a candidate's profile chose not to hire the candidate based on what they found." *Id.* Melinda J. Caterine & Peter F. Herzog, *The Government Cares About My Profile? Latest Trends In Federal Regulation Of Social Media: Latest Employer Concerns With Respect To Regulation Of Social Media*, 2012 A.B.A. SEC'Y. OF LABOR & EMPL. LAW, 6TH ANN. LABOR & EMPL. LAW CONF. 4, *available at* http://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2012/acpapers/13A.authcheckdam.pdf.

[7] Kelly Jackson Higgins, *No Passwords, PINs For Most Smartphone And Tablet Users*, DARKREADING (Sept. 29, 2011, 4:36 PM), http://www.darkreading.com/insider-threat/167801100/security/news/231602443/no-passwords-pins-for-most-smartphone-and-tablet-users.html; Kate Rogers, *Help! My Boss Friend Requested Me on Facebook*, FOX BUS.: SMALL BUS. CENTER (Mar. 29, 2012), http://smallbusiness.foxbusiness.com/legal-hr/2012/03/29/help-my-boss-friend-requested-me-on-facebook/; Martha C. White, *Facebook Weighs In and Blasts 'Shoulder Surfing' by Employers*, TIME: BUS. & MONEY, Mar. 23, 2012, http://business.time.com/2012/03/23/facebook-weighs-in-and-blasts-shoulder-surfing-by-employers/#ixzz2HAEeN9sd.

likened them to "requiring someone's house keys."[8]

The configuration of social media websites typically permits users to choose between various methods of communication to interact. These choices enable users to dictate the parameters of their audiences.[9] To use Facebook as an example, contrast the public elements of "Timeline Posts" and "Open Graph Concepts" with the "private messaging" feature.[10] Analogous features—"Tweets" and "Direct Messages," respectively—exist on Twitter.[11] It is conceded that by choosing forms of communication that are not configured to be private, users forfeit any expectation of privacy with respect to such communications. Regarding publicly disseminated content, social media users interact at their own risk. But communications that are configured to be private are not ordinarily subject to public scrutiny. When employers and academic institutions coerce applicants to divulge passwords to access private communications, they invade realms of privacy that should be subject to more exacting protection. Consistent with the Electronic Communications Privacy Act, Congress should adopt a configuration-based approach to delineating protected zones of privacy with respect to password-protected social media, personal online accounts, and personal communications devices.[12]

Part I discusses the Stored Communications Act (the "SCA"), its purpose, and unauthorized activity thereunder.[13] The recent decisions rendered in *Pietrylo v. Hillstone Restaurant Group* and *Pure Power Boot Camp v. Warrior Fitness Boot Camp* will be highlighted to show how courts have interpreted the SCA in the context of employment relations.[14] Part II illustrates the potential for employment

[8] Singletary, *supra* note 2.

[9] Margaret Rouse, *Definition: Facebook*, WHATIS.COM, http://whatis.techtarget.com/definition/Facebook (last updated Feb. 2009) ("A member can make all his communications visible to everyone, he can block specific connections or he can keep all his communications private. Members can choose whether or not to be searchable, decide which parts of their profile are public, decide what not to put in their newsfeed and determine exactly who can see their posts. For those members who wish to use Facebook to communicate privately, there is a message feature, which closely resembles email.").

[10] *Id*. *See* Catharine Smith & Bianca Bosker, *What Not To Post on Facebook: 13 Things You Shouldn't Tell Your Facebook Friends*, HUFFINGTON POST, Nov. 1, 2010, http://www.huffingtonpost.com/2010/11/01/what-not-to-post-on-facebook_n_764338.html#s157112&title=Your_Birth_Date; *Open Graph Overview*, FACEBOOK DEVELOPERS, https://developers.facebook.com/docs/concepts/opengraph/ (last updated Feb. 22, 2013).

[11] About Tweets (Twitter Updates), Twitter, https://support.twitter.com/groups/31-twitter-basics/topics/109-tweets-messages/articles/127856-about-tweets-twitter-updates (last visited Feb. 22, 2013); How to Post and Delete Direct Messages (DMs), Twitter, https://support.twitter.com/groups/31-twitter-basics/topics/109-tweets-messages/articles/14606-how-to-post-and-delete-direct-messages-dms (last visited Feb. 22, 2013).

[12] *See infra* notes 20–21 and accompanying text.

[13] 18 U.S.C. §§ 2701–12 (2012).

[14] Pietrylo v. Hillstone Rest. Grp., No. 06–5754 (FSH), 2009 WL 3128420 (D. N.J. Sept. 25, 2009); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

discrimination by employers who demand access to personal social media. Part III compares state statutes that forbid employers and educational institutions from demanding passwords and prevent retaliation against employees and students who refuse to divulge their passwords. Part III also examines the Password Protection Act of 2012 (the "PPA") and the Social Networking Online Protection Act (the "SNOPA"), two failed federal bills aimed at providing password protection.[15] Throughout the comparative analysis, Part III will be geared toward identifying the most well-crafted provisions of current state legislation so that Congress can draft an effective password protection bill.

I. THE STORED COMMUNICATIONS ACT

In 1986, Congress passed the Electronic Communications Privacy Act (the "ECPA"), which was intended to afford privacy protection to electronic communications.[16] Title II of the ECPA created the Stored Communications Act, and it addresses access to stored wire and electronic communications and transactional records.[17] The SCA makes it an offense to "intentionally access[ ] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ ] . . . access to a wire or electronic communication while it is in electronic storage in such system."[18] The SCA excludes from liability, however, "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user."[19]

The legislative history of the ECPA indicates that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards.[20] The drafting Committee intended that the configuration of an electronic communications system would determine whether or not an electronic communication was readily accessible to the public.[21] Password protection legislation would effectuate this intent by prohibiting employers from accessing the private features of applicants' accounts. Publicly accessible material, such as unrestricted "Timeline Posts" (on Facebook) and "Tweets" (on Twitter), would remain unprotected.[22]

---

[15] Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/hr5684; Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012), *available at* http://www.govtrack.us/congress/bills/112/hr5050#.

[16] 18 U.S.C. §§ 2510–22.

[17] S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[18] 18 U.S.C. § 2701(a)(1).

[19] *Id.* § 2701(c)(2).

[20] S. REP. NO. 99-541, at 35 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public.").

[21] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002).

[22] *See* Rouse, *supra* note 9; *About Tweets*, *supra* note 11; *How to Post and Delete Direct*

In *Pure Power Bootcamp v. Warrior Fitness Bootcamp*, an employee's (Alexander Fell's) Hotmail username and password were made available on his employer's work computer via the web-browser's "auto fill" function.[23] Auto fill is a function of Internet software that stores information previously entered, such as passwords, to prevent the user from having to input such information every time he wants to access a particular website or service.[24] When someone accessed the Hotmail website, Fell's login information was automatically entered in the login screen.[25] When other employees discovered this, they accessed Fell's Hotmail account during working hours and provided hard copies of several e-mails to his supervisor.[26] The Southern District of New York held that Fell's employer violated the SCA because it "intentionally" accessed Fell's e-mail account without valid authorization.[27]

In *Pietrylo v. Hillstone Restaurant Group*, the District Court of New Jersey ruled that social networking sites, as well as private groups and sections contained therein, are subject to the SCA.[28] In that case, two employees (Brian Pietrylo and Doreen Marino) of Houston's created a private, invitation-only, password-protected MySpace "Spec-Tator" group for their co-workers.[29] The employees made derogatory comments about management and customers.[30] No managers were invited to join.[31] However, one manager became aware of the site when an employee named St. Jean showed it to him.[32] Houston's managers twice asked St. Jean for her username and password, and she willingly provided it without indicating any reservations.[33] The managers then accessed the group on five occasions "before firing the site's creators for damaging employee morale and for violating the restaurant's 'core values.'"[34] The plaintiffs alleged, *inter alia*, that the managers accessed the "Spec-Tator" group without authorization in violation of the SCA.[35]

Messages (DMs), *supra* note 11.

[23] Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

[24] Sarah Brown, *What is Auto Fill?*, EHOW TECH, http://www.ehow.com/facts_6775539_auto-fill_.html (last visited Mar. 14, 2013).

[25] Caterine & Herzog, *supra* note 6.

[26] *Id.*

[27] *Id.*

[28] *See* Pietrylo v. Hillstone Rest. Grp., No. 06–5754 (FSH), 2009 WL 3128420 (D. N.J. Sept. 25, 2009).

[29] Brian Hall, *Court Upholds Jury Verdict in* Pietrylo v. Hillstone Restaurant Group, EMPLOYER LAW REPORT (Oct. 19, 2009), http://www.employerlawreport.com/2009/10/articles/workplace-privacy/court-upholds-jury-verdict-in-pietrylo-v-hillstone-restaurant-group/#axzz2GxbaL414.

[30] *Id.*

[31] *Id.*

[32] *Pietrylo*, 2009 WL 3128420, at *3.

[33] *Id.*

[34] Hall, *supra* note 29.

[35] *Pietrylo*, 2009 WL 3128420, at *2.

Relying on St. Jean's testimony that she both felt compelled to give out her password because she thought that if she failed to comply, she "probably would have gotten in trouble," and that she would not have given up her password if a manager had not been the one to make the request, the District Court held that "[t]he jury could reasonably infer from such testimony that St. Jean's purported 'authorization' was coerced or provided under pressure. As a result, this testimony provided a basis for the jury to infer that Houston's accessing of the Spec-Tator was not, in fact, authorized."[36]

The *Pure Power* case lends persuasive authority to the proposition that an employer who accesses an employee's personal password-protected e-mail account, which is maintained by an outside electronic communication service provider, violates the SCA if such access is without authorization. The *Pietrylo* decision counsels employers not to tamper with employees' passwords because even if consent to access a password-protected account is seemingly provided, a jury could find that valid authorization was not in fact given, and damages may ensue.[37] An employer holding out an employment opportunity has significant leverage vis-à-vis a job applicant or employee who is reluctant to divulge his or her password. Faced with the prospect of losing an employment opportunity or the approval of an interviewer, a job applicant will likely acquiesce to the employer's demands and divulge his or her password. Current employees, similar to St. Jean in *Pietrylo*, may also experience undue pressures for fear of losing their jobs. As one Illinois Institute of Technology student stated, "[e]specially in times like this when there are not a lot of jobs, that puts a lot of pressure on you. It's hard to resist."[38] In light of the above opinions and the courts' attitudes toward employers accessing employees' private electronic communications, more comprehensive and prohibitive legislation is needed in order to afford protection to electronic communications that are configured to be private.

II. EMPLOYMENT DISCRIMINATION IMPLICATIONS

Title VII of the Civil Rights Act of 1964 made it unlawful for an employer "to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual . . . because of such individual's race, color, religion, sex, or national origin."[39] The Civil Rights Act of 1991 (the "CRA of 1991") amended Title VII by adding §

[36] *Id.* at *3.
[37] *Id.*
[38] *Now illegal for Illinois Employers to Ask for Facebook Logins*, FOX NEWS (Aug. 1, 2012), http://www.foxnews.com/us/2012/08/01/now-illegal-for-illinois-employers-to-ask-for-facebook-logins/.
[39] 42 U.S.C. § 2000e-2(a) (2012).

2000e-2(m) (the "motivating factor provision"), which states that "[e]xcept as otherwise provided in this subchapter, an unlawful employment practice is established when the complaining party demonstrates that race, color, religion, sex, or national origin was a motivating factor for any employment practice, even though other factors also motivated the practice."[40]

In order to prevail on a claim of disparate treatment prior to passage of the 1991 amendments, a Title VII complainant was required to prove that the legitimate reasons offered by his or her employer for an adverse employment decision were not the employer's true motivation, but rather, a pretext for discrimination.[41] The words "because of" in Title VII were interpreted as invoking the concept of "but-for" causation, or necessity.[42] The *McDonnell Douglas-Burdine* framework—the original theory of relief under Title VII—instructed courts to apply the restrictive "but-for" causation requirement to the issue of whether an employer's consideration of protected characteristics caused an adverse employment decision.[43] Under a system where "but-for" causation must be demonstrated in order to prove a violation of Title VII, employers are permitted to use protected characteristics such as race or sex in their decision-making so long as such discrimination does not rise to the level of necessity.[44] One commentator argues that utilization of protected characteristics that goes undeterred by the law for failing to rise to the "but-for" level causes social harm by increasing both the risk that minorities will suffer discriminatory harm and the likelihood of future utilization of protected characteristics by employers.[45]

---

[40] *Id.* § 2000e-2(m). "Courts analyze Title VII cases using two theories formulated by the Supreme Court—disparate treatment and disparate impact." Susan Melanie Jones, *Applying Disparate Impact Theory to Subjective Employee Selection Procedures*, 20 LOY. L.A. L. REV. 375–76, 389 (1987). Instead of the disparate impact model, which focuses on the effects of an employment procedure, the disparate treatment model, which addresses intentional discrimination, is the focus of the following discussion because disparate treatment bears more directly on the question of whether employers should be allowed to use the subjective screening methods addressed herein.

[41] McDonnell Douglas Corp. v. Green, 411 U.S. 792, 804 (1973). A pretext is "a reason given in justification of a course of action that is not the real reason." *Pretext*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/english/pretext?q=pretext (last visited Mar. 14, 2013).

[42] Price Waterhouse v. Hopkins, 490 U.S. 228, 262 (1989) (O'Connor, J., concurring) ("The legislative history of Title VII bears out what its plain language suggests: a substantive violation of the statute only occurs when consideration of an illegitimate criterion is the 'but-for' cause of an adverse employment action. The legislative history makes it clear that Congress was attempting to eradicate discriminatory actions in the employment setting, not mere discriminatory thoughts.").

[43] Texas Dep't of Cmty. Affairs v. Burdine, 450 U.S. 248 (1981); *McDonnell Douglas Corp.*, 411 U.S. 792; Martin J. Katz, *The Fundamental Incoherence of Title VII: Making Sense of Causation In Disparate Treatment Law*, 94 GEO. L.J. 489, 500 (2006).

[44] Katz, *supra* note 43, at 494.

[45] *Id.* at 519–20.

The CRA of 1991 expanded Title VII by establishing a less restrictive causal threshold for plaintiffs to satisfy in order to obtain relief for employment discrimination.[46] Whereas fact finders in *McDonnell Douglas-Burdine* pretext cases seek to discern a single predominating motive by evaluating whether proffered motives are real or pretext, mixed-motive analysis is employed where it has been shown that an employment decision resulted from a mixture of legitimate and illegitimate motives.[47] Congress entitled the motivating factor provision: "Clarifying Prohibition against impermissible consideration of race, color, religion, sex, or national origin in employment practices."[48] This title and the CRA of 1991's legislative history reaffirm that Title VII was meant to prohibit *all* invidious consideration of sex, race, color, religion, or national origin in employment decisions, and that *any* reliance on prejudice in making employment decisions is illegal.[49] In contrast to the restrictive "but-for" requirement implicit in Title VII's original prohibition against employment discrimination, commentators have interpreted the motivating factor language in the 1991 amendments as invoking the concept of "minimal causation."[50] Minimal causation is satisfied where factors have some influence on an employment decision, but do not rise to the level of necessity or sufficiency.[51] Thus, the use of a protected characteristic as a "motivating factor" or a consideration in the decision constitutes an illegal employment practice. This suggests that the causal nexus between the consideration of a protected characteristic and an adverse employment decision need not be so dispositive as to constitute necessity or sufficiency.[52] Rather, a plaintiff need only "demonstrate" a

[46] Through the CRA of 1991, Congress intended "to strengthen existing protections and remedies available under federal civil rights laws to provide more effective deterrence and adequate compensation for victims of discrimination." H.R. REP. NO. 102-40 (1991), *reprinted in* 1991 U.S.C.C.A.N. 694, 694.

[47] *Price Waterhouse*, 490 U.S. at 232. The CRA of 1991 was largely motivated by the perceived hostility towards civil rights reflected in the Supreme Court's 1989 split decision in *Price Waterhouse*. Benjamin C. Mizer, *Toward a Motivating Factor Test for Individual Disparate Treatment Claims*, 100 MICH. L. REV. 234, 238 (2001). The *Price Waterhouse* plurality held that once a plaintiff in a Title VII case shows that gender influenced an employment decision, the defendant could avoid liability only by proving that it would have made the same decision even if it had not improperly considered the employee's gender. *Price Waterhouse*, 490 U.S. at 245. The CRA of 1991 partially codified *Price Waterhouse* by adopting the motivating factor test endorsed by the majority. 42 U.S.C. § 2000e-2(m) (2012). The Act also partially overruled the holding in *Price Waterhouse* in that it does not allow employers to escape liability altogether by asserting the same-decision defense. Under the 1991 amendments, if the plaintiff proves a violation under the motivating factor provision but the defendant succeeds on the same-decision defense, the plaintiff is entitled to limited relief. *Id.* § 2000e-5(g)(2)(B).

[48] 42 U.S.C. § 2000e-2(m).

[49] H.R. REP. NO. 102-40 (1991), *reprinted in* 1991 U.S.C.C.A.N. 694, 695, 710.

[50] Katz, *supra* note 43, at 505–06; *see* Mizer, *supra* note 47, at 250.

[51] Katz, *supra* note 43, at 505.

[52] 42 U.S.C. § 2000e-2(m).

minimally causal relationship.[53]

Despite the expansion of Title VII and the broad construction of civil rights laws generally,[54] it has been suggested that Title VII is inadequate to effectively deter consideration of protected characteristics, and improvements need to be made with respect to the punitive and deterrent sanctions that attach with liability in mixed-motive cases.[55] To the extent that Congress is serious about prohibiting discrimination in the workplace, greater protections must be implemented in order to prevent employers from accessing private online information and using such information to unlawfully discriminate against employees.

Employers who access password-protected social media run the risk of violating Title VII because social media are replete with information relating to employees' and applicants' membership in protected classes. Privately configured messages can reveal protected characteristics that are not immediately apparent to employers, and they can also reveal characteristics that employers are prohibited from inquiring about, such as religion and national origin. Allowing employers unfettered access to applicants' social media substantially increases the risk that they will illegally consider impermissible criteria while making employment decisions.[56] Federal password protection legislation would mitigate this risk by limiting the information upon which employers may base their decisions to that which is publicly available. By restricting employers' access to protected information, they will be deterred from using illicit information as motivating factors for their employment decisions, and thus be forced to use more restricted and legitimate methods to conduct pre-employment screening.

---

[53] *Id.*

[54] "The evils against which [Title VII] is aimed are defined broadly . . . . Accordingly, under longstanding principles of statutory construction, the Act should 'be given a liberal interpretation . . . .'" Int'l Bhd. of Teamsters v. United States, 431 U.S. 324, 381 (1977) (Marshall, J., concurring in part and dissenting in part).

[55] Under the same action provision, where an employer prevails on a same action defense, only injunctive relief and attorneys' fees are available to the plaintiff. 42 U.S.C. § 2000e-5(g)(2)(B). Yet injunctive relief, which cannot include orders to hire or reinstate under § 2000e-5(g)(2)(B), is costless to the employer, and courts have tended to limit attorneys' fees in "same action" cases. Katz, *supra* note 43, at 539. "[I]f we are serious about enforcing the norm against utilization of protected characteristics, and rely heavily upon a private attorneys general model to enforce this norm, Congress should provide better incentives for plaintiffs in minimal causation cases to act as private attorneys general." *Id.* at 540.

[56] Subjective evaluation processes offer a strong potential for discriminatory abuse because they give employers broad discretion. Employers who do not recognize their own prejudices may abuse that discretion unintentionally. Jones, *supra* note 40, at 418–19; *see* Erin Egan (Chief Privacy Officer), *Protecting Your Passwords and Your Privacy*, FACEBOOK (Mar. 23, 2012, 5:32 AM), https://www.facebook.com/note.php?note_id=326598317390057 ("Employers . . . may not have the proper policies and training for reviewers to handle private information.").

III. PASSWORD PROTECTION LEGISLATION AT THE STATE AND FEDERAL LEVELS: A COMPARATIVE ANALYSIS

Six states—California, Delaware, Illinois, Maryland, Michigan, and New Jersey—enacted laws in 2012 that prohibit requesting or requiring an employee, applicant or student to disclose a user name or password for a personal social media account.[57] Two similar bills, the Password Protection Act of 2012 and the Social Networking Online Protection Act, were introduced in Congress and died without making it past the committee phase.[58] Comparing state and Congressional approaches in this area should be useful to lawmakers seeking a blueprint of provisions for successful legislation. The scope, terminology, operative provisions, and exceptions of these statutes highlight the values involved and the mechanisms that states have employed to protect them.

Congress must determine the parameters of forthcoming password protection legislation. Maryland and Illinois have prohibited employers, but not educational institutions, from requesting passwords.[59] The PPA took a similar approach.[60] In contrast, Delaware and New Jersey have prohibited institutions of higher education, but not employers, from requesting the passwords of students and applicants for admission.[61] California and Michigan's laws are the most inclusive with respect to the contexts that they regulate—both of those states prohibit password solicitation by employers as well as educational institutions.[62] Michigan's education law is broader than those passed in Delaware, New Jersey, and California because the latter three apply only to postsecondary institutions, whereas Michigan's statute applies to public and private schools at all levels of instruction.[63] The SNOPA would

---

[57] *Employer Access to Social Media Usernames and Passwords*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 17, 2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.

[58] Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012); Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).

[59] 820 ILL. COMP. STAT. 55 / 10 (2012); MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012).

[60] H.R. 5684.

[61] DEL. CODE ANN. tit. 14, §§ 8101–05 (West 2012); Assemb. B. 2879, 215th Leg. (N.J. 2012).

[62] CAL. LAB. CODE § 980 (West 2012); CAL. EDUC. CODE §§ 99120–22 (West 2012); Internet Privacy Protection Act, H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012).

[63] Delaware's Education Privacy Act, DEL. CODE ANN. tit. 14, § 8102 (West 2012), defines "[a]cademic institution" as a "public or nonpublic institution of higher education or institution of postsecondary education"; New Jersey's Assemb. B. 2879 applies to "[p]ublic or private institution[s] of higher education"; California's §§ 99120–22 apply to "[p]ublic and private postsecondary educational institutions"; and Michigan's Internet Privacy Protection Act, H.R. 5523, reads:

> "Educational institution" means a public or private educational institution or a separate school or department of a public or private educational institution, and includes an academy; elementary or secondary school; extension course; kindergarten; nursery school; school system; school district; intermediate school district; business, nursing, professional, secretarial, technical, or vocational school; public or private educational

have applied to employers as well as institutions of higher education.[64] The risks of invalid authorization, discrimination, and "chilling" important discourse discussed herein are present in both the employment and academic contexts. Accordingly, Congress should adopt the approach of Michigan's Internet Privacy Protection Act to secure password protection for employees and students at all levels of academic institutions.[65]

Congress must also develop a coherent set of terminology so that the law is properly inclusive and can achieve its desired outcome. Perhaps one of the reasons that the PPA failed to become law is that the bill did not precisely define what content would be protected. The PPA sought to amend the Computer Fraud and Abuse Act (the "CFAA"), a law that has been widely criticized for vagueness.[66] The PPA borrowed language from the CFAA in that it sought to prohibit employers from compelling or coercing any person to authorize access to a "protected computer" that is not the employer's "protected computer."[67] The CFAA defines "protected computer" broadly as a computer

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[68]

The states' statutes provide considerable guidance on what language may be better used to safeguard employees' expectations of privacy with respect to electronic communications. California's employment and education laws prohibit employers and educational institutions from requiring or requesting employees and students to divulge user names and passwords for "personal social media."[69]

---

testing service or administrator; and an agent of an educational institution. Educational institution shall be construed broadly to include public and private institutions of higher education to the greatest extent consistent with constitutional limitations.

64 Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).

65 H.R. 5523; Peter Micek, *New Senate Bill Targets Snooping Bosses*, ACCESS (May 9, 2012, 5:24 PM), https://www.accessnow.org/blog/new-senate-bill-targets-snooping-bosses ("Students deserve the same protection from their schools that this bill provides to employees in their jobs.").

66 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012); Password Protection Act of 2012, H.R. 5684, 112th Cong. § 2(a) (2012) ("Section 1030(a) of title 18, United States Code, is amended . . . ."); *see generally* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010).

67 H.R. 5684.

68 18 U.S.C. § 1030(e)(2).

69 CAL. LAB. CODE § 980 (West 2012); CAL. EDUC. CODE §§ 99120–22 (West 2012). In both

Illinois and Delaware's prohibitions pertain to requesting employees to provide passwords to their accounts or profiles on social networking websites.[70] Curiously, however, Illinois explicitly excludes e-mail from its definition of "social networking website."[71] Michigan prohibits employers and educational institutions from requesting information that allows access to or observation of an individual's "personal internet account."[72] Delaware, New Jersey, and Maryland all focus on the means of access; each of those states prohibits access to certain material through "electronic communication devices."[73] The New Jersey and Maryland statutes use identical terminology in that they both protect "personal account[s] or service[s]."[74] The SNOPA would have made it unlawful for employers and institutions of higher education to require or request user names, passwords, or any other means for accessing "private email account[s]" or "personal account[s] . . . on any social networking website."[75] The language chosen by the state legislatures suggests that the problems discussed herein transcend social media, and that protection should extend to personal e-mail accounts, personal electronic communications devices, and personal social media.[76]

Another issue that is explicitly addressed by some, but not all, of these statutes is the phenomenon of "shoulder surfing" during job

statutes, "social media" means an electronic service or account, or electronic content, including but not limited to, videos or still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations.

[70] 820 ILL. COMP. STAT. 55 / 10 (2012) ("'[S]ocial networking website' means an Internet-based service that allows individuals to: (A) construct a public or semi-public profile within a bounded system, created by the service; (B) create a list of other users with whom they share a connection within the system; and (C) view and navigate their list of connections and those made by others within the system."); DEL. CODE ANN. tit. 14, § 8102 (West 2012) ("'Social networking site' means an internet-based, personalized, privacy-protected website or application whether free or commercial that allows users to construct a private or semi-private profile site within a bounded system, create a list of other system users who are granted reciprocal access to the individual's profile site, send and receive email, and share personal content, communications, and contacts.").

[71] 820 ILL. COMP. STAT. 55 /10 ("'Social networking website' shall not include electronic mail.").

[72] Internet Privacy Protection Act, H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012) ("'Personal internet account' means an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data.").

[73] MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); DEL. CODE ANN. TIT. 14, § 8103 (West 2012); Assemb. B. 2879, 215th Leg. (N.J. 2012).

[74] MD. CODE ANN., LAB. & EMPL. § 3-712; Assemb. B. 2879.

[75] Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).

[76] The compilation of suggested protected materials reflects a synthesis of the state and Congressional approaches to this area. This synthesis is meant to encompass not just social media accounts, but a broad class of password-protected material on the Internet and on personal devices, including e-mail accounts and smart phone applications containing sensitive banking and financial information. Users of password-encrypted websites should enjoy an expectation of privacy in the information they seek to protect.

interviews.[77] Shoulder surfing occurs when an interviewer demands that someone access their personal account in the interviewer's presence in order to examine the password-protected features of the account.[78] In addition to prohibiting requests for passwords, the California and Delaware password protection laws each contain separate provisions prohibiting requests that job applicants access password-protected material in the presence of an employer or school official.[79] Michigan's law addresses the issue by including the clause, "allow observation of," in its operative provisions.[80] The New Jersey and Illinois statutes prohibit shoulder surfing less explicitly—New Jersey prohibits schools from requiring students or applicants to "in any way provide access to" protected material, and Illinois prohibits employers from "demand[ing] access in any manner" to an employee's or prospective employee's social networking account.[81] It is debatable whether the SNOPA or Maryland statutes addressed the issue at all. Maryland prohibits employers from requiring employees to disclose user names, passwords, "or other means for accessing" protected material, and the SNOPA similarly would have prohibited compelled disclosure of "any other means" for accessing protected material.[82] The PPA failed to address shoulder surfing as a separate category of prohibited conduct. Instead, it sought to prohibit employers from compelling or coercing individuals to "authorize access, such as by providing a password or similar information through which a computer may be accessed" to protected computers.[83] The reality is that the undesired conduct at issue in this Note—access by employers and school officials to password-protected material—may be achieved through multiple techniques. Any attempt to eradicate the undesired conduct must effectively deter all methods of engaging in such conduct. An employer may request a password so that he can access password-protected material, or he may instead "shoulder surf" so as to escape liability under poorly crafted legislation. In order to unequivocally proscribe all methods of accessing password-protected

[77] White, *supra* note 7.

[78] *Id.*

[79] *E.g.*, CAL. LAB. CODE § 980 (West 2012) ("An employer shall not require or request an employee or applicant for employment to . . . [a]ccess personal social media in the presence of the employer"); DEL. CODE ANN. tit. 14, § 8103(b) (West 2012) ("An academic institution shall not require or request that a student or applicant log onto a social networking site, mail account, or any other internet site or application by way of an electronic communication device in the presence of an agent of the institution so as to provide the institution access.").

[80] Internet Privacy Protection Act, H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012) ("An employer shall not . . . [r]equest an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account.").

[81] 820 ILL. COMP. STAT. 55 / 10 (2012); Assem. B. 2879, 215th Leg. (N.J. 2012).

[82] MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012); Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).

[83] Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012).

material, Congress must prohibit demands for passwords, as well as demands for individuals to access private material in the presence of those who are prohibited from viewing it.

With the exception of Illinois' law, the state statutes discussed in this section, the PPA, and the SNOPA all contain "no retaliation" provisions that prohibit employers or academic institutions from taking retaliatory action against an individual who fails or refuses to comply with a request or demand for access to password-protected material.[84] "No retaliation" provisions enhance the efficacy of password-protection legislation by establishing that employers and schools are not only prohibited from requesting or demanding access to password-protected material, but they are also prohibited from taking retaliatory action against an individual. Separately from the remedies and penalties that may be provided for, Congress would be well-advised to include a similar "no retaliation" provision in forthcoming legislation so that employers and academic institutions are given clear notice that they cannot pressure individuals to divulge password-protected material. This would enable employees and students to feel secure and protected when they refuse to comply with illegal requests.

Password-protected social media accounts present challenging issues for lawmakers because not all such accounts are appropriately classified as "personal" accounts.[85] Many entities make concerted efforts to have a strong online presence, and thus, through their employees, they maintain profiles and accounts on social networking websites.[86] Some lawyers argue that proprietary sites are akin to exclusive information, and therefore, they can and should be protected and controlled by the company.[87] In order to appropriately deal with issues such as the treatment of company-owned online representations that are created and managed by individual employees, employer-issued electronic devices, law enforcement issues, and other privacy concerns, forthcoming legislation must contain precise exceptions and special provisions. The PPA, for example, contained an exception allowing courts to grant equitable relief where "there are specific and articulable facts providing reasonable grounds to believe that the information sought to be obtained is relevant and material to protecting the intellectual property . . . of the party seeking the relief."[88] The PPA also provided that its prohibitions may be waived by state law with respect to state government employees who work with individuals under the

[84] *See* 820 ILL. COMP. STAT. 55 / 10; *infra* Table 1 for a compilation of these provisions.

[85] Benjamin L. Riddle, *Passwords, Privacy and Protection – The Social Networking Online Protection Act*, NATIONAL LAW REVIEW (Aug. 21, 2012), http://www.natlawreview.com/article/passwords-privacy-and-protection-social-networking-online-protection-act.

[86] *Id.*

[87] *Id.*

[88] H.R. 5684, 112th Cong. § 2(d)(2)(A).

age of thirteen and by executive agencies dealing with classified information.[89] California's employment law contains exceptions allowing access to employer-issued electronic devices and personal social media "reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding."[90] California's education law requires postsecondary educational institutions to post their social media privacy policies on their websites.[91] The Education Privacy Act of Delaware contains a relatively broad set of special prohibitions. Under that statute, academic institutions are forbidden from

> monitor[ing] or track[ing] a student's or applicant's personal electronic communication device . . . request[ing] or requir[ing] a student or applicant to add [school] . . . representative[s] to their personal social networking site profile or account . . . [and] accessing a student's or applicant's social networking site profile or account indirectly through any other person who is a social networking contact of the student or applicant.[92]

Michigan's law contains exceptions that allow access to electronic communication devices paid for in whole or in part by employers or educational institutions, accounts or services provided by employers or educational institutions or obtained by virtue of the individual's relationship with the employer or the educational institution, and, in certain circumstances, information that is necessary to ensure compliance with laws, regulations, and prohibitions against work-related misconduct.[93] New Jersey's law prohibits educational institutions from inquiring whether a student or applicant has an account or profile on a social networking website, and it also prohibits them from requiring students or applicants to waive or limit any protection thereunder.[94] Maryland's law contains exceptions that permit access to non-personal accounts or services that provide access to the employer's internal computer or information systems, and the law allows investigations under limited circumstances.[95] Unlike the PPA and the other state statutes, the Illinois statute and the SNOPA do not contain any exceptions or special prohibitive provisions.[96] If Congress revisits

89 *Id.* § 2(d)(B)(ii–iii).
90 CAL. LAB. CODE § 980 (West 2012).
91 CAL. EDUC. CODE §§ 99120–22 (West 2012).
92 DEL. CODE ANN. tit. 14, § 8103 (West 2012).
93 Internet Privacy Protection Act, H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012).
94 Assemb. B. 2879, 215th Leg. (N.J. 2012).
95 MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012).
96 *See* 820 ILL. COMP. STAT. 55 / 10 (2012); *see also* Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).

the issue of nationwide password protection, it may decide to draw from these exceptions in order to draft sound legislation. Congress must carefully balance personal privacy interests against numerous countervailing interests maintained by the government, employers, and educational institutions in order to develop narrow and limited exceptions to any prohibitions it establishes.[97]

CONCLUSION

Password-protected social media are often configured to simultaneously allow users to broadcast their ideas to global audiences and to communicate privately with others. Federal password protection legislation would serve to supplement and improve existing laws pertaining to protection of stored wire and electronic communications, unauthorized access, and employment discrimination, while promoting a healthy public forum for important discourse on social media websites by students and employees. Although six states have adopted measures granting password protection for students and employees, Congress has twice failed to enact similar protections. Congress must act promptly to protect not just social media, but also e-mail, financial information, personal communication devices, and other personal password-protected material against overzealous employers and academic institutions. Forthcoming legislation should proscribe requests or demands for passwords, as well as requests or demands for individuals to access password-protected material in the presence of employers or school representatives. Moreover, it should prohibit retaliation against individuals who refuse to comply with any such requests or demands. State legislation must guide lawmakers in drafting legislation that will protect the privacy of both employees and students without being overly broad or under-inclusive. Careful drafting and precise statutory terminology will provide effective and measured relief for this problem.

*Timothy J. Buckley**

Table 1: Retaliation Provisions	
Statutes	**"No Retaliation" Language**
California CAL. LAB. CODE § 980 (West 2012); CAL.	"An employer shall not discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section"; "A

[97] Riddle, *supra* note 85.

[*] *Articles Editor*, CARDOZO ARTS & ENT. L.J. Vol. 32, J.D. candidate, Benjamin N. Cardozo School of Law (2014); B.S., SUNY Oneonta. Special thanks to Professor Arthur Jacobson, Charles Finocchiaro, and my devoted parents, Joanne and George Buckley.

EDUC. CODE §§ 99120–22 (West 2012)	public or private postsecondary educational institution shall not suspend, expel, discipline, threaten to take any of those actions, or otherwise penalize a student, prospective student, or student group in any way for refusing to comply with a request or demand that violates this section."
Delaware DEL. CODE ANN. tit. 14, § 8104 (West 2012)	"An academic institution may not discipline, dismiss or otherwise penalize or threaten to discipline, dismiss or otherwise penalize a student for refusing to disclose any information specified in § 8103(a) or (b) of this title. It shall also be unlawful for a public or nonpublic academic institution to fail or refuse to admit any applicant as a result of the applicant's refusal to disclose any information specified in § 8103(a) or (b) of this title."
Michigan Internet Privacy Protection Act, H.R. 5523, 96th Leg., Reg. Sess. (Mich. 2012)	"An employer shall not . . . [d]ischarge, discipline, fail to hire, or otherwise penalize an employee or applicant for employment for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account. . . . An educational institution shall not . . . [e]xpel, discipline, fail to admit, or otherwise penalize a student or prospective student for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the student's or prospective student's personal internet account."
New Jersey Assem. B. 2879, 215th Leg. (N.J. 2012)	"No public or private institution of higher education in this State shall . . . [p]rohibit a student or applicant from participating in activities sanctioned by the institution of higher education, or in any other way discriminate or retaliate against a student or applicant, as a result of the student or applicant refusing to provide or disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device as provided in subsection a. of this section."
Maryland MD. CODE ANN., LAB. & EMPL. § 3-712 (West 2012)	"An employer may not: (1) discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose any information specified in subsection (b)(1) of this section; or (2) fail or refuse to hire any applicant as a result of the applicant's refusal to disclose any information specified in subsection (b)(1) of this section."
Congress Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012); Social Networking Online Protection Act, H.R. 5050, 112th	" . . . discharges, disciplines, discriminates against in any manner, or threatens to take any such action against, any person-- (i) for failing to authorize access described in subparagraph (A) to a protected computer that is not the employer's protected computer; or (ii) who has filed any complaint or instituted or caused to be instituted any proceeding under or related to this paragraph, or has testified or is about to testify in any such proceeding"; "It shall be unlawful for any employer . . . (2) to discharge, discipline, discriminate against in any manner, or deny employment or

Cong. (2012)	promotion to, or threaten to take any such action against, any employee or applicant for employment because-- (A) the employee or applicant for employment refuses or declines to provide a user name, password, or other means for accessing a private email account of the employee or applicant or the personal account of the employee or applicant on any social networking website; or (B) such employee or applicant for employment has filed any complaint or instituted or caused to be instituted any proceeding under or related to this Act or has testified or is about to testify in any such proceeding."