

Journal of Business & Technology Law


Volume 9 | Issue 1

Article 8

Maryland's Social Networking Law: No "Friend" to Employers and Employees

Alexander Borman

Follow this and additional works at: <http://digitalcommons.law.umaryland.edu/jbtl>

 Part of the [Administrative Law Commons](#), [Business Administration, Management, and Operations Commons](#), [Business Law, Public Responsibility, and Ethics Commons](#), [Business Organizations Law Commons](#), [Communications Law Commons](#), [Communication Technology and New Media Commons](#), [Consumer Protection Law Commons](#), [Education Law Commons](#), [Entrepreneurial and Small Business Operations Commons](#), [Fourth Amendment Commons](#), [Interpersonal and Small Group Communication Commons](#), [Legislation Commons](#), [Operations and Supply Chain Management Commons](#), [Organizational Behavior and Theory Commons](#), [Privacy Law Commons](#), [Science and Technology Law Commons](#), and the [Strategic Management Policy Commons](#)

Recommended Citation

Alexander Borman, *Maryland's Social Networking Law: No "Friend" to Employers and Employees*, 9 J. Bus. & Tech. L. 127 (2014)
Available at: <http://digitalcommons.law.umaryland.edu/jbtl/vol9/iss1/8>

This Notes & Comments is brought to you for free and open access by the Academic Journals at DigitalCommons@UM Carey Law. It has been accepted for inclusion in Journal of Business & Technology Law by an authorized editor of DigitalCommons@UM Carey Law. For more information, please contact smccarty@law.umaryland.edu.

Maryland's Social Networking Law: No "Friend" to Employers and Employees

I. INTRODUCTION

WHEN HE SIGNED SENATE BILL 433 on May 2, 2012, Governor Martin O'Malley made Maryland the first state in the nation to legally prohibit employers from requesting or requiring an employee or job applicant to disclose their user name or password to access a social networking account.¹ Many states have passed, or are currently considering passing laws to protect employees from being forced to provide their usernames and passwords to social networking websites, commonly referred to as "social networking laws."² As of October 2013, social networking laws have been instituted or are currently pending in thirty-six states.³ Additionally, efforts to ban the practice nationwide have gained traction in Congress through such legislation as the Social Networking Online Protection Act (SNOPA) and the Password Protection Act.⁴ Maryland's social networking law does not explicitly resolve several major issues surrounding the use of social networking in the context of the employer-employee relationship. Ensuring that both employers and

© 2014 Alexander Borman

* J.D., University of Maryland Francis King Carey School of Law, Dec. 2013; Master of Public Policy, University of Maryland School of Public Policy, Dec. 2013; B.A. Political Science & Economics, St. Mary's College of Maryland, May 2010. Thank you to the editors of the *Journal of Business & Technology Law* for their help throughout the publication process. Also, a special thanks to Daniel and Christine for their boundless support.

1. Joanne Deschenaux, *Maryland Enacts Country's First Social Media Password Law*, SOCIETY FOR HUMAN RESOURCE MANAGEMENT (May 3, 2012), <http://www.shrm.org/LegalIssues/StateandLocalResources/Pages/MarylandEnactsCountryFirst.aspx>.

2. See, e.g., Scott Paulson, *Illinois Employees 'Like' Gov. Quinn's New Social Networking Law*, EXAMINER.COM (Aug. 2, 2012), <http://www.examiner.com/article/illinois-employees-like-gov-quinn-s-new-social-networking-law>.

3. *Employer Access to Social Media Usernames and Passwords: 2013 Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES (NCSL) (Oct. 23, 2013), <http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx> [hereinafter NCSL, 2013 Legislation].

4. Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013); Password Protection Act of 2013, H.R. 2077, 113th Cong. (2013); see also Michelle Maltais, *SNOPA Bill Seeks to Keep Employers Out of Private Social Networks*, LOS ANGELES TIMES (Apr. 30, 2012), <http://articles.latimes.com/2012/apr/30/business/la-fi-tn-federal-bill-bans-employers-seeking-facebook-password-20120430>.

employees are clearly and adequately protected requires lawmakers to modify Maryland's social networking law.

Section II of this comment will provide necessary background information, including a definition of what constitutes "social networking." Section III will explore the legal environment in Maryland before the social networking law was passed, the events that led to its passage, and the language of the law.⁵ Section IV will examine how other states and the federal government has implemented social networking laws. Section V, the legal analysis section, will examine potential issues with the law as well as solutions to fix the law's loopholes and ambiguities. These issues include: (1) how the social networking law may affect due diligence in hiring; (2) loopholes in the law that hinder its effectiveness; (3) the absence of penalties; (4) the non-applicability of the law to certain accounts; and (5) the lack of protection for relationships between "educational" employees, i.e. students, and their schools. Section VI will conclude with some final thoughts on Maryland's social networking law.

II. SOCIAL NETWORKING AND PRIVACY

Social networking sites have become a ubiquitous part of the internet and people's daily lives. However, the explosion in popularity of social networking websites has led to a multitude of problems within the employer-employee relationship. As of March 31, 2013, Facebook had 1.11 billion people logging in to its website every month.⁶ Facebook is just one of many social networking sites that are available to people who use the internet. A "social networking site" is "[a] Web site that provides a venue for people to share their activities with family, friends and colleagues or to share their interest in a particular topic."⁷ People can use social networking sites to share photos, post their thoughts, and send messages to other people in a method analogous to sending an email. Some of the most popular social networking sites include Facebook, Twitter, Myspace, LinkedIn, and Google Plus.⁸

5. In the interest of brevity, this comment will not examine the First Amendment implications of Maryland's social networking law. Instead, the comment will narrowly focus on the intention of Maryland's social networking law to prevent employers from accessing employees' social networking accounts.

6. *Number of Active Users at Facebook Over the Years*, THE ASSOCIATED PRESS (May 1, 2013), <http://news.yahoo.com/number-active-users-facebook-over-230449748.html>.

7. *Definition of Social Networking Site*, PC MAGAZINE, http://www.pcmag.com/encyclopedia_term/0,2542,t=social%2Bnetworking&ti=55316,00.asp (last visited Nov. 9, 2013).

8. See FACEBOOK, www.facebook.com (last visited Nov. 9, 2013) (a popular U.S. social networking website); TWITTER, www.twitter.com (last visited Nov. 9, 2013) (website utilizes 140-character messages); MYSPACE, www.myspace.com (last visited Nov. 9, 2013) (website has a strong focus on music and was one of the original social networking websites); LINKEDIN, www.linkedin.com (last visited Nov. 9, 2013) (website emphasizes career connections) ; GOOGLE+, <https://plus.google.com/> (last visited Nov. 9, 2013) (website interfaces with Google's Gmail internet service).

The complication that arises from social networking sites is that social networking sites provide users with differing amounts of privacy depending on the user's personal preferences as well as the functions of the particular social networking site that they are using. For example, a user on Facebook can post information that they can choose to make available to anyone on the social networking site or choose to make only available to their "friends," people who are granted access to view a person's profile after specifically requesting access.⁹ The information available on social networking sites can be categorized into three broad categories of information based on how private the user wants the information to be: (1) public information that is available to anyone online; (2) semi-private information that is restricted to a group of "friends" or "friend of friends"; and (3) private information such as instant chat messages and internal site messaging, similar to emails.¹⁰

With the different categories of privacy, users can become confused about what information is available to others when they provide that information on their social networking page. This confusion has led to a variety of legal issues. In personal injury cases, insurance claims adjusters have searched social networking sites to find information that showed a plaintiff snowboarding who claimed he was injured in a car accident.¹¹ In employment law, employers have fired employees who have used social media to disparage their employers or fellow employees.¹²

9. See FACEBOOK, www.facebook.com (last visited Nov. 9, 2013).

10. Evan E. North, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. KAN. L. REV. 1279, 1288 (2010). Facebook switched everyone's individual email on the site to an "@Facebook.com" email address. Samantha Murphy Kelly, *Facebook Switched Your Email to One You've Probably Never Used*, MASHABLE SOCIAL MEDIA (Jun. 25, 2012), <http://mashable.com/2012/06/25/facebook-email-address/>. By doing so, Facebook has expanded the private information available online.

11. North, *supra* note 10, at 1279.

12. Josh Eidelson, *Can You Be Fired For What You Post on Facebook?*, SLATE.COM (July 3, 2012), http://www.slate.com/articles/news_and_politics/jurisprudence/2012/07/getting_fired_for_what_you_post_on_facebook.html. Four employees of Hispanics United of Buffalo (HUB) were fired by HUB under the company's harassment policy. The employees had started and participated in a Facebook message thread. The workers successfully appealed their case to the NLRB, but are currently awaiting an appeal from that judgment. *Id.* Employers must tread carefully as well when vetting applicants using social media. An employer may expose itself to liability through Title VII if a rejected applicant can prove that an employer utilized gender, race, national origin, or religion in their hiring decision. See Megan Whitehill, *Better Safe Than Subjective: The Problematic Intersection of Pre-Hire Social Networking Checks and Title VII Employment Discrimination*, 85 TEMP. L. REV. 229, 229 (2012).

III. HISTORY AND STRUCTURE OF MARYLAND'S SOCIAL NETWORKING LAW

A. *The Previous State of the Law*

Maryland legislators have previously passed laws to safeguard the private information that is held by businesses. Maryland's Personal Information Protection Act (PIPA) mandates that businesses protect personal information from unauthorized access.¹³ Businesses cannot escape this requirement by contracting its information security needs to a third party.¹⁴ Failure to follow a provision of PIPA subjects the violator to both criminal and civil liability via Maryland's Consumer Protection Act.¹⁵ However, before Maryland's social networking law was implemented, Maryland's laws did not protect prospective or current employees from being forced to provide employers their social networking usernames and passwords.

The State of Maryland's demand of a prospective correctional officer to provide his Facebook login and password provided the motivation for Maryland's social networking law.¹⁶ There are no other publicly reported cases in Maryland where an employer asked for access to a person's social networking account.¹⁷ There are various explanations that may account for this fact. First, it is possible that employers rarely ask employees for their social networking username and passwords.¹⁸ With so much of the information on social networking sites publically available to an employer through a simple internet search, an employer may not find it necessary to ask an employee or prospective employee for their login credentials.

Another explanation is that employees and prospective employees are afraid to report employers who ask for such information in fear of losing their current or future job. As is detailed *infra*, it was the acknowledgement of this fear that led

13. MD. CODE ANN., COM. LAW § 14-3502(b) (West 2013).

14. COM. LAW § 14-3503(b)(1).

15. COM. LAW § 14-3508. *See also* MD. CODE ANN., COM. LAW §§ 13-410, 13-411 (West 2013).

16. *See infra* Part III.B.

17. However, *USA Today* details the experiences of a New York City statistician as well as other state, county, and local governments who asked for employees' social networking log-in information. Shannon McFarland, *Job Seekers Getting Asked for Facebook Passwords*, USA TODAY (Mar. 21, 2012), <http://usatoday30.usatoday.com/tech/news/story/2012-03-20/job-applicants-facebook/53665606/1>.

18. This explanation was advocated by Nick Fishman, co-founder of EmployeeScreenIQ, an employment screening company. Nick Fishman, *Should Employers Ask Candidates for Their Facebook Passwords?*, TLNT (May 7, 2013), <http://www.tlnt.com/2013/05/07/should-employers-ask-candidates-for-their-facebook-passwords/>. *See also* Kirsten Korosec, *Can a Prospective Employer ask for your Facebook Password?*, SMARTPLANET (Jan. 3, 2013), <http://www.smartplanet.com/blog/bulletin/can-a-prospective-employer-ask-for-your-facebook-password/9366> (noting that "[t]he password requests haven't become a mainstay in human resource departments nationwide yet").

Maryland correctional officer Robert Collins to speak out against the practice.¹⁹ Correctional and police officers, who might be expected to consent to access to their social networking in the name of public safety, may be the most commonly asked for their social networking information.²⁰ However, correctional and police office may be the least likely to file a complaint. It is common practice for police departments to check an applicant's public social networking page and some departments, including the Virginia State Police, readily admit that they also check the private web pages of applicants.²¹ The Virginia State Police, in defending their policy, state that "in today's society, the virtual character check is just as important as the 'physical' character check."²² Moreover, multiple police departments within Maryland require a polygraph that extensively checks an applicant's background.²³ The information revealed by a polygraph is even more intimate as it may examine thoughts and acts that the employee never intended to share. With such revealing information already required, it is possible that police officers have little concern when asked for their social networking information.²⁴

Courts in Maryland and the Fourth Circuit have rarely had the opportunity to consider social networking, much less access to a person's social networking login information, in their judicial decisions. When social networking has been considered, it is often in the context of proper authentication of information from social networking sites.²⁵ The most well-known case in Maryland is that of *Griffin v. State*, in which the Maryland Court of Appeals ruled that information from social networking websites used in trials must be properly authenticated.²⁶ One of the only cases in the Fourth Circuit relating to the privacy of social networking information

19. See *infra* Part III.B.

20. See generally Tyra M. Vaughn, *Public Safety Agencies Use Social Media to Check Applicants' Backgrounds*, DAILY PRESS (Sept. 1, 2012), http://articles.dailypress.com/2012-09-01/news/dp-nws-police-hires-facebook-background-checks-0823-20120901_1_social-media-wight-sheriff-mark-marshall-check-job.

21. *Id.*

22. *Id.*

23. See, e.g., *Anne Arundel County Entry Level Police Officer Processing Information*, http://www.aacounty.org/Personnel/Resources/PD_Processing_Information.pdf (requiring a polygraph examination); *Montgomery County, MD Sheriff's Office: Minimum Qualifications*, <http://mcsheriff.com/minimum-qualifications/> (last visited Nov. 11, 2013) (stating that the application process "requires a psychological evaluation, medical exam and a drug screening and polygraph or other deception detection examination."); *Ocean City Police Department Medical Requirements*, http://oceancitymd.gov/Police/police_employment.html (last visited Nov. 11, 2013) (stating that candidates must successfully complete a polygraph examination).

24. It is also possible that speaking out against such requirements could cost police officers their job. The intimidation of employees and their inability to say "no" when employers ask for their social networking usernames and passwords was one of the primary impetuses for Maryland's social networking law. See *infra* Part III.B.

25. See, e.g., *Griffin v. State*, 419 Md. 343, 427 (2011).

26. *Id.*

is *Bland v. Roberts*.²⁷ In *Bland*, the Fourth Circuit Court of Appeals found that a deputy sheriff's lawsuit for wrongful termination filed after being fired for "liking" the Facebook page of the sheriff's opponent should go to trial because a "like" is constitutionally protected speech.²⁸

B. History of Maryland's Social Networking Law

Senator Ronald Young, the Maryland senator who introduced Senate Bill 433, was originally inspired to sponsor the bill after he learned of job applicants who felt forced to hand over their social networking usernames and passwords when asked by prospective employers.²⁹ Senator Young compared the practice to "asking to go into your house and read your mail and listen to your phone calls."³⁰ Delegate Shawn Tarrant, one of the bill's sponsors in the House of Delegates, similarly equated asking for employee's social networking login information to phone eavesdropping.³¹

The incident that directly led to the formation and implementation of Senate Bill 433 originated with Robert Collins, an officer with the Maryland Department of Corrections.³² After his mother died, he took a leave of absence and later applied for his previous job in 2010.³³ During a security interview, the Department of Corrections asked for his Facebook username and password, implying that his employment was conditional on him providing that information.³⁴ When Mr. Collins asked them why they needed the information, his employer responded that the information was necessary to ensure that Mr. Collins was not a member of nor

27. 730 F.3d 368 (4th Cir. 2013).

28. *Id.* at 385–386. To "like" something on Facebook is to show others that one "enjoy[s]" a person, place, or thing by connecting to the object's page. *Id.* It is important to note that this case would be unaffected by a social networking law as the sheriff, the deputy sheriff's supervisor, did not ask for or receive the deputy sheriff's social networking login information as the "like" was publicly available information. *See generally* *Bland v. Roberts*, 857 F.Supp.2d 599, 603–04 (E.D.Va. 2012).

29. Ben Giles, *Maryland Bans Employers From Asking for Facebook Passwords*, WASHINGTON EXAMINER (May 2, 2012), <http://washingtonexaminer.com/maryland-bans-employers-from-asking-for-facebook-passwords/article/564481#.UFzvtY1IRnQ>.

30. *Id.*

31. Kevin Rector, *Maryland Becomes First State to Ban Employers From Asking for Social Media Passwords*, THE BALTIMORE SUN (Apr. 10, 2012), http://articles.baltimoresun.com/2012-04-10/news/bs-md-privacy-law-20120410_1_facebook-password-social-media-bradley-shear.

32. *See id.*; *Resume, Cover Letter And Your Facebook Password?*, NATIONAL PUBLIC RADIO (Mar. 21, 2012), <http://www.npr.org/2012/03/21/149091139/resume-cover-letter-and-your-facebook-password>.

33. Doug Gross, *ACLU: Facebook Password Isn't Your Boss' Business*, CNN (Mar. 22, 2012), http://articles.cnn.com/2012-03-22/tech/tech_social-media_facebook-password-employers_1_facebook-password-aclu-facebook-facebook-s-terms?_s=PM:TECH.

34. *Id.*

affiliated with a gang.³⁵ Mr. Collins stated that he “reluctantly gave him the password” because he “really needed the job.”³⁶

Mr. Collins contacted the American Civil Liberties Union (ACLU) for assistance before even driving away after his interview.³⁷ On January 25, 2011, the ACLU sent a letter to the Maryland Department of Public Safety and Correctional Services requesting that the Department of Corrections stop requesting the user names and passwords of social networking sites while conducting background checks.³⁸ In response to the ACLU’s letter, Gary Maynard, Maryland Secretary of Public Safety, suspended the department’s employment policy regarding social networking for 45 days as of February 22, 2011.³⁹ On April 6, 2011, Secretary Maynard sent a letter to the ACLU explaining the department’s new employment policy regarding social networking.⁴⁰ The new social networking policy mandated that applicants sign a form stating that they understand that it is voluntary for them to provide their credentials to their social networking accounts.⁴¹ Although corrections officials would previously examine the social networking pages without the employee present, the new policy would allow employees to examine their social networking accounts with the interviewer.⁴²

Despite the new policy, the ACLU was still unsatisfied with the coercive nature of the employee social networking policy and the intrusion of privacy not only of the applicant, but also of the applicant’s social networking connections.⁴³ However, the alleged coercive nature of the policy was partially belied by the fact that all five employees, out of eighty, who refused access to their social networking accounts

35. *Id.*

36. *Id.*

37. Ategh Khaki, *Status Update: Employers Asking For Your Facebook Password Violates Your Privacy and the Privacy of All Your Friends, Too*, ACLU BLOG OF RIGHTS (Mar. 22, 2012, 2:49 PM), <http://www.aclu.org/blog/technology-and-liberty/status-update-employers-asking-your-facebook-password-violates-your>.

38. Letter from Deborah A. Jeon, Legal Director, American Civil Liberties Union of Maryland, to Gary D. Maynard, Secretary, Maryland Department of Public Safety and Correctional Services, (Jan. 25, 2011), http://www.aclu-md.org/uploaded_files/0000/0041/letter-_collins_final.pdf.

39. Letter from Gary D. Maynard, Secretary, Maryland Department of Public Safety and Correctional Services, to Sara N. Love, President, American Civil Liberties Union of Maryland, (Feb. 22, 2011), http://www.aclu-md.org/uploaded_files/0000/0042/letter-_doc_suspends_policy_for_45_days.pdf.

40. Press Release, American Civil Liberties Union of Maryland, *ACLU Says Division of Corrections’ Revised Social Media Policy Remains Coercive and Violates “Friends” Privacy Rights* (Apr. 18, 2011), http://www.aclu-md.org/press_room/30.

41. *Id.*

42. *Id.*

43. *Id.*

during their previous three hiring cycles, were hired.⁴⁴ The Department of Corrections indicated that it denied employment to seven of the 2,689 applicants whose social networking accounts they reviewed.⁴⁵ The Department of Corrections denied these individuals employment because “[a]ll seven of these individuals’ social media applications contained pictures of them showing verified gang signs (signs commonly known to law enforcement which are utilized by gangs)”⁴⁶

The ACLU used the experience of Mr. Collins as the impetus to advocate for a law in Maryland that would prohibit employers from asking employees and applicants to share their username and passwords to their social networking accounts.⁴⁷ The ACLU mounted an extensive media campaign to highlight Mr. Collin’s experience that garnered national attention.⁴⁸ A bill prohibiting employers from asking employees about their social networking user names and passwords passed the Maryland State Senate and Maryland House of Delegates “with almost unanimous support” in April 2012.⁴⁹

C. Structure of Maryland’s Social Networking Law

Maryland’s social networking law consists of two components. The first and primary component of the Act regulates employers’ access to user names and passwords.⁵⁰ The Act prohibits an employer from “request[ing] or requir[ing] that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device.”⁵¹ The Act also prohibits any retaliation against an employee or an applicant

44. Bob Sullivan, *Govt. Agencies, Colleges Demand Applicants’ Facebook Passwords*, MSNBC (Mar. 6, 2012), http://redtape.nbcnews.com/_news/2012/03/06/10585353-govt-agencies-colleges-demand-applicants-facebook-passwords?lite.

45. *Id.*

46. *Id.*

47. See *HB 964 – Labor and Employment – User Name and Password Privacy Protection: Hearings Before the Maryland House Economic Matters Committee*, 2012 Leg., 430 Sess. (Md. 2012) (testimony by the American Civil Liberties Union), http://www.aclu-md.org/uploaded_files/0000/0179/hb_964_facebook_testimony.pdf.

48. See, e.g., Tim Persinko & Chris Gordon, *Job Applicant Required to Give Facebook Login: ACLU*, NBC 4 WASHINGTON (Feb. 22, 2011), <http://www.nbcwashington.com/news/tech/DC-Job-Applicant-Required-to-Give-Facebook-Password-ACLU-116655589.html>; Megan Garber, *Would You Give Job Interviewers Your Facebook Password? Because They Might Ask*, THE ATLANTIC (Mar. 20, 2012), <http://www.theatlantic.com/technology/archive/2012/03/would-you-give-job-interviewers-your-facebook-password-because-they-might-ask/254810/>; ACLU Maryland, *Want a Job? Password, Please!*, YOUTUBE (Feb. 10, 2011), <http://www.youtube.com/watch?v=bDaX5DTmbfY>.

49. Meredith Bennett-Smith, *Job Interviewer Asks For Facebook Password. Should You Give It?*, THE CHRISTIAN SCIENCE MONITOR (June 11, 2012), <http://www.csmonitor.com/Business/2012/0611/Job-interviewer-asks-for-Facebook-password.-Should-you-give-it>.

50. MD. CODE ANN., LAB. & EMPL. § 3-712(b) & (c) (West 2013).

51. LAB. & EMPL. § 3-712(b)(1).

if they refuse to provide their account username or password.⁵² However, the Act provides an exception that requires employees to disclose their user names and passwords to the employer's internal computer system.⁵³

The second component clarifies that the law is not meant to stifle investigations into regulatory violations and investigations into unauthorized use of proprietary information or financial data.⁵⁴ This component enables an employer to investigate instances of employee wrongdoing utilizing methods that would otherwise be prohibited by Maryland's social networking law. Employees are specifically prohibited by the law from "download[ing] unauthorized employer proprietary information or financial data."⁵⁵ After an employer receives information about an employee using a non-business account for business purposes, an employer is allowed to investigate "for the purpose of ensuring compliance with applicable securities or financial law, or regulatory requirements . . ."⁵⁶ Additionally, the Act allows a company to investigate an employee when the employer receives information about the "unauthorized downloading of an employer's proprietary information or financial data."⁵⁷

In May 2013, the Maryland legislature approved enforcement provisions for the social networking law.⁵⁸ The added provisions state that if the Maryland Commissioner of Labor and Industry determines that the social networking law has been violated, the Commissioner will "(i) try to resolve any issue involved in the violation informally by mediation; or (ii) ask the Attorney General to bring an action on behalf of the applicant or employee."⁵⁹ Furthermore, the additional provision authorizes the Maryland Attorney General to bring a court action for relief when there is an alleged violation of the law.⁶⁰

Maryland's social networking law is not narrowly tailored to social networking despite the impetus for the act, as explained *supra*, involving the social networking website Facebook.⁶¹ The Act not only applies to an employee's or applicant's user name or password to a social networking site, but also to their username and password to *any* "personal account or service through an electronic communications device."⁶² The Act defines "electronic communications device" as

-
- 52. LAB. & EMPL. § 3-712(c).
 - 53. LAB. & EMPL. § 3-712(b)(2).
 - 54. LAB. & EMPL. § 3-712(d) & (e).
 - 55. LAB. & EMPL. § 3-712(d).
 - 56. LAB. & EMPL. § 3-712(e)(1).
 - 57. LAB. & EMPL. § 3-712(e)(2).
 - 58. S.B. 305, 2013 Leg., 431st Sess. (Md. 2013).
 - 59. LAB. & EMPL. § 3-712(f)(1).
 - 60. LAB. & EMPL. § 3-712(f)(2).
 - 61. See *supra* Part III.B.
 - 62. LAB. & EMPL. § 3-712(b)(1).

including “computers, telephones, personal digital assistants, and other similar devices.”⁶³ The Act’s inclusive definition protects an employee or applicant from having to reveal the user name and password to their social networking, email, voicemail, and financial accounts.⁶⁴ Therefore, although the Act may have been publicized as a law to protect social networking accounts, the law has broad applications beyond social networking.⁶⁵

IV. COMPARISONS OF MARYLAND’S SOCIAL NETWORKING LAW

A. Regulation on the State Level

Although Maryland was the first state in the nation to pass a law preventing employers from requesting access to employees’ social networking accounts,⁶⁶ other states have followed Maryland’s lead in passing similar legislation. By the end of January 2013, these states included California, Delaware, New Jersey, Michigan, and Illinois.⁶⁷ However, only eight months later, states including Arkansas, Colorado, Nevada, New Mexico, Oregon, Utah, Vermont, and Washington passed laws protecting the privacy rights of employees.⁶⁸ Furthermore, as of October 2013, approximately thirty-six states are currently considering passing legislation regulating employers’ access to employees’ social networking accounts.⁶⁹

Of the social networking laws that have been enacted, only the social networking laws of approximately half of the states can be deemed “comprehensive” social networking laws as they apply to the employer-employee relationship as well as the university-student relationship.⁷⁰ In July 2012, Delaware became the first state that explicitly prohibits both public and nonpublic academic institutions from

63. LAB. & EMPL. § 3-712(a)(3)(ii).

64. This illustrative list of accounts was created by the Act’s prohibition of employer access to a personal account or service through an “electronic communication device.” LAB. & EMPL. § 3-712(b)(1). The Act defines an electronic communication device as “any device that uses electronic signals to create, transmit, and receive information.” LAB. & EMPL. § 3-712(a)(3)(i). The affected devices range from those specified in the Act including “computers, telephones, personal digital assistants, and other similar devices.” LAB. & EMPL. § 3-712(a)(3)(ii). The language in the Act would also likely cover new technologies such as Google Glass.

65. This comment only explores the controversy surrounding social networking.

66. See Deschenaux, *supra* note 1.

67. See Jessica Holdman, *Lawmakers Divided Over Social Media Privacy Legislation*, THE BISMARCK TRIBUNE (Jan. 29, 2013), http://bismarcktribune.com/business/local/lawmakers-divided-over-social-media-privacy-legislation/article_0b6d0158-6a71-11e2-a724-0019bb2963f4.html.

68. See NCSL, *2013 Legislation*, *supra* note 3.

69. NCSL, *2013 Legislation*, *supra* note 3.

70. These states include California, Michigan, Delaware, Arkansas, Illinois, New Jersey, New Mexico, and Oregon. *Employer Access to Social Media Usernames and Passwords: 2012 Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 17, 2013), <http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx>.

requesting the login information to or monitoring the social networking accounts of students and applicants.⁷¹ California followed shortly thereafter by passing similar legislation in September 2012.⁷² Delaware's legislation, in contrast to California's legislation,⁷³ is notable for the fact that it applies to schools from elementary schools through universities.⁷⁴ This is distinct from Maryland's proposed athlete monitoring law, originally utilized by Delaware as a template,⁷⁵ which was limited only to "postsecondary institutions."⁷⁶

B. Regulation on the Federal Level

The federal Social Networking Online Protection Act (SNOPA) addresses many of the same issues that Maryland's social networking law sought to address regarding employers requesting access to employees' social networking user names and passwords. Specifically, SNOPA would prevent employers and universities from requiring employees and students, respectively, to provide their username and passwords to any social networking site.⁷⁷ However, some courts have found that the federal Stored Communications Act (SCA) already protects employees from employers who access their social networking and email accounts without their permission. The SCA makes it illegal for a person to:

- (1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or

71. Michelle Maltais, *Student Social Media Privacy bill Passes Delaware Legislature*, LOS ANGELES TIMES (July 2, 2012), <http://www.latimes.com/business/technology/la-student-social-media-privacy-bill-graduates-in-delaware-20120702,0,5471704.story?track=rss>. See 2012 DEL. CODE ANN. tit. 14, §8103(a) & (b) (2012) (banning the practice of shoulder-surfing and requiring the student or applicant to connect to the university's social networking page).

72. Dina Abou Salem, *California First to Endorse Comprehensive Social Media Privacy Law*, ABC 7 (Dec. 27 2012), <http://abcnews.go.com/blogs/headlines/2012/12/california-first-to-endorse-comprehensive-social-media-privacy-law/>.

73. *Id.*

74. Tit. 14, § 8103.

75. Bradley Shear, *Shear on Social Media Law: Delaware Passes Student-Athlete Social Media Privacy Legislation*, SHEAR ON SOCIAL MEDIA LAW (July 3, 2012), <http://www.shearsocialmedia.com/2012/07/delaware-passes-student-athlete-social.html>. Subsequent bills providing students with social media privacy rights failed to pass in the 2013 session. *Session Highlights: Legislation That Failed to Pass*, MARYLAND INDEPENDENT COLLEGE AND UNIVERSITY ASSOCIATION (MICUA), <http://www.micua.org/legislative-update/session-highlights> (last visited Nov. 9, 2013).

76. S.B. 434, 2012 Leg., 430th Sess. (Md. 2012).

77. Renee Radia, *Social Networking Online Protection Act Seeks to Protect Privacy*, E-MARKETING ASSOCIATES (May 2, 2012), <http://www.e-marketingassociates.com/social-networking-online-protection-act-seeks-to-protect-privacy/>.

(2) intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system.⁷⁸

The SCA, which was initially added to Title 18 in 1986, was founded during a time when online social networking websites did not exist.⁷⁹ Congress created the SCA “to prevent hackers from obtaining, altering or destroying certain stored electronic communications.”⁸⁰ Despite its origins, the SCA has periodically been used to prevent unauthorized access to social networking and other online accounts. After finding a violation of the SCA, a jury in the U.S. District Court for the District of New Jersey ruled in favor of employees of Houston’s Restaurant who were fired after an employer gained access to their private chat group by asking an employee for their password.⁸¹ Notably, the employer never directly threatened the employee with termination or any type of adverse employment action if the employee did not relinquish their password.⁸² Conversely, the same court found no violation of the SCA when a coworker, who was friends with the plaintiff on Facebook, took a screenshot of the plaintiff’s offensive wall post and sent the screenshot to the employer “completely unsolicited.”⁸³

Federal courts have also applied protections through SCA to email accounts corresponding to what SNOA would accomplish. In the U.S. District Court for the Southern District of New York, the court found a violation of the SCA where an employer gained access to an employee’s email accounts by using the employee’s personal account information that was stored on the company network.⁸⁴ Additionally, in *Cardinal Health 414, Inc. v. Adams*, a U.S. District Court held that a violation of the SCA occurred where a former employee used the usernames and passwords of current employees to login to their email accounts.⁸⁵

These cases may demonstrate that SNOA is not necessary to address the issue of employers seeking out the user names and passwords of employees. However, cases

78. Stored Communications Act, 18 U.S.C.A. §2701 (West 2013).

79. *Id.*

80. In re DoubleClick Inc. Privacy Litigation, 154 F.Supp.2d 497, 507 (S.D.N.Y. 2001).

81. See Pietrylo v. Hillstone Restaurant Group, No. 06-5754 (FSH), 2008 WL 6085437, at *3, (D. NJ July 25, 2008); see also Phillip L. Gordon, *Verdict Against Houston’s Restaurant Demonstrates Risks of Accessing Employee’s Restricted Social Networking Sites*, LITTLER MENDELSON P.C. (July 14, 2009), <http://www.littler.com/publication-press/publication/verdict-against-houstons-restaurant-demonstrates-risks-accessing-emplo>.

82. *Pietrylo*, 2008 WL 6085437, at *3. The U.S. District Court for the Eastern District of Pennsylvania also found the SCA applicable to Facebook. *Rodriguez v. Widener University*, Civil Action No. 13-1336, 2013 WL 3009736, at *9 (E.D.Pa. June 17, 2013).

83. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, Civ. No. 2:11-cv-03305 (WJM), 2013 WL 4436539, at *9, (D. NJ Aug. 20, 2013).

84. *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F.Supp.2d 548, 551-52 (S.D.N.Y. 2008).

85. 582 F.Supp.2d 967, 977 (2008).

such as *Castle Megastore Grp., Inc. v. Wilson* provide cause for concern.⁸⁶ In *Wilson*, the U.S. District Court for Arizona held there was insufficient evidence to support the finding that a Facebook page qualified for protection under the SCA.⁸⁷ The comprehensive protection offered by SNOPA would ensure that people's private information is protected and would also prevent incongruent rulings nationwide.

V. LEGAL IMPLICATIONS

Maryland's social networking law contains many ambiguities and loopholes that limit its effectiveness. The first ambiguity involves due diligence in hiring/retention.⁸⁸ Employers may be misled to believe that due diligence in hiring no longer requires an employer to search the social networking accounts of employees and prospective employees. However, an employer may still be legally liable for detrimental information that is publically available. Next, loopholes exist regarding alternative methods of accessing social networking information.⁸⁹ Under Maryland law, employers may still have the option to gain access to the social networking accounts of employees and prospective employees using such methods as connecting with the employee on the social networking site with the purpose of enabling the employer to view an individual's private profile. Third, the law does not contain penalties.⁹⁰ Maryland's social networking law provides no civil or criminal penalties for the violation of any of its provisions. Without clear penalties, violations of the law are more likely to occur. Fourth, the law does not apply to work accounts.⁹¹ The new law only applies to an employee's "personal" account. The failure of the law to define what type of account constitutes a "personal" account enables employers to liberally access employees' work email as well as accounts linked to that email. Finally, the law lacks protections for students.⁹² The text and legislative history of Maryland's social networking law both establish that students are not included in the definition of protected persons. However, pervasive monitoring of students' social networking, in particular the monitoring of student-athletes, suggests that students require the same protection as employees and prospective employees.

86. No. CV-12-02101-PHX-DGC, 2013 WL 672895 (D.Ariz Feb. 25, 2013).

87. *Id.* at *2.

88. *See infra* Part V.A.

89. *See infra* Part V.B.

90. *See infra* Part V.C.

91. *See infra* Part V.D.

92. *See infra* Part V.E.

A. Due Diligence

When employers seek to hire an employee, they often desire applicants who exhibit traits such as professionalism, confidence, and intellectual curiosity.⁹³ In finding an employee who meets those qualifications, the employer must make sure to use due diligence. In *Athas v. Hill*, the Maryland Court of Special Appeals explained that “it is the duty of an employer to use due diligence in the selection of competent and careful employees and in the retention in its service of none but those who are.”⁹⁴ Additionally, the court specified that an employer cannot legally delegate or relieve itself of its responsibility to use due diligence.⁹⁵ Without further expanding on the notion, the Maryland Court of Appeals recognized that a party could possibly bring a negligence claim when an employer fails to use due diligence.⁹⁶ Bringing forth a claim in Maryland courts for negligently hiring an employee requires five elements.⁹⁷ These five elements are:

- (1) that the individual was employed by defendant employer,
- (2) that individual employee was incompetent,
- (3) defendant employer had actual or constructive knowledge of that incompetence,
- (4) an individual employee’s act or omission caused the plaintiff’s injury, and
- (5) that defendant employer’s negligence in hiring or retaining individual was the proximate cause of the plaintiff’s injury.⁹⁸

The most important element to focus on, in the context of Maryland’s social networking law, is the third element. The law in Maryland before the social networking law came into effect likely required that “due diligence,” as recognized by Maryland Courts in the hiring of new employees, compelled a company to conduct an online search of the candidate before hiring them. In *Evans v. Morsell*, decided in 1978, the Maryland Court of Appeals declined to hold an employer responsible for conducting a background check partially because of the burden it would put on employers.⁹⁹ In contrast, a background check today can be completed

93. Meghan Casserly, *Top Five Personality Traits Employers Hire Most*, FORBES (Oct. 4, 2012), <http://www.forbes.com/sites/meghancasserly/2012/10/04/top-five-personality-traits-employers-hire-most/>.

94. *Athas v. Hill*, 54 Md.App. 293, 295, 458, A.2d 859, 861 (1983), *aff’d*, 300 Md. 133, 476 A.2d 710 (1984).

95. *Id.*

96. *Evans v. Morsell*, 284 Md. 160, 165, 395 A.2d 480, 483 (1978).

97. *Harris v. Creative Hairdressers, Inc.*, No. Civ. JFM-04-1992, 2005 WL 2138128, at *2 (D.Md. Sept. 2, 2005).

98. *Id.* (citing *McGuiness v. Brink’s Inc.*, 60 F.Supp.2d 496, 501 (D.Md.1999). “Actual knowledge” refers to what an employer actually knows. According to Black’s Law Dictionary, it is defined as “[d]irect and clear knowledge.” *Black’s Law Dictionary* (9th ed. 2009), available at Westlaw Next BLACKS. “Constructive knowledge” refers to “[k]nowledge that one using reasonable care of diligence should have False” *Id.*

99. *Evans*, 395 A.2d at 484.

online by a wide variety of companies with little effort.¹⁰⁰ However, with even less effort, an employer can conduct a free internet search of an employee or job applicant and find a plethora of information about them, including information from their social networking accounts.¹⁰¹ A survey conducted in early 2012 by the website CareerBuilder found that 37% of surveyed companies stated that they research job applicants on social networking websites.¹⁰² While searching the social networking accounts of prospective employees, a large minority of employers have reported finding information that led to them not hiring a prospective employee.¹⁰³ Such information includes prospective employees posting provocative or inappropriate photographs and information, content about the job candidates' drug and alcohol use, and job candidates who post negative information about previous employers.¹⁰⁴

Although Maryland's social networking law was crafted to protect employers from liability, the law could instead cause businesses to contend with unexpected liability because of the requirements of due diligence. Bradley Shear, an attorney who specializes in social media law,¹⁰⁵ claims that employers under Maryland's social networking law are now relieved of the responsibility from any knowledge gained from accessing an employee's social networking website.¹⁰⁶ Shear provides the example of a company discovering from an employee's social networking website that the employee is unstable, and he describes the employer's subsequent legal requirement to "take action and/or monitor their employee's activities."¹⁰⁷ However, a plaintiff suing an employer in court could make the argument that even if an employer is not required under Maryland's social networking law to access the employee's private social networking website, the employer is still obligated to conduct a simple internet search and access the employee's public social networking website. If detrimental information is discoverable in a quick search, a company

100. For example, companies like US Search and PeopleSmart require only a person's last name to conduct an instant background check. See US SEARCH, www.ussearch.com (last visited Nov. 10, 2013); PEOPLESMART, <http://www.peoplesmart.com> (last visited Nov. 10, 2013).

101. See Rosemary Haefner, *More Employers Screening Candidates via Social Networking Sites*, CAREERBUILDER.COM (June 10, 2009), <http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/>.

102. Vicki Salemi, *Hiring Managers Admit to Surfing Job Seekers' Social Media Profiles*, MEDIA JOBS DAILY (Apr. 24, 2012), http://www.mediabistro.com/mediajobsdaily/hiring-managers-admit-to-surfing-job-seekers-social-media-profiles_b10773.

103. Haefner, *supra* note 101.

104. Haefner, *supra* note 101.

105. *Law Office of Bradley S. Shear: Attorney Profile*, http://shearlaw.com/attorney_profile (last visited Nov. 10, 2013).

106. Kenneth Artz, *Maryland Law Protects Social Networking Passwords*, THE HEARTLAND INSTITUTE (July 9, 2012), <http://news.heartland.org/newspaper-article/2012/07/09/maryland-law-protects-social-networking-passwords>.

107. *Id.*

may have no less of a legal obligation than they would have had before the law was passed, under Maryland's requirement of due diligence, to access that information.

B. Workarounds to Meet the Letter, but not the Spirit of the Law

Although Maryland's social networking law prevents employers from requesting individuals' usernames and passwords to their private social networking accounts, the law does not prevent employers from using a variety of different techniques to access their private social networking accounts. As mentioned previously, employers are legally able and may be legally required to access publically available information on employees' and prospective employees' social networking websites.¹⁰⁸ Employers have a menu of options in front of them to access applicants' social networking information that are not prohibited under Maryland's social networking law. The options available to employers include: 1) connecting with the employee through the social networking site to enable the employer to view their profile;¹⁰⁹ 2) physically standing behind an employee after they have entered in their social networking username and password and then forcing them to explore their social networking profile;¹¹⁰ and 3) requiring an employee to change their privacy settings to make their social networking profile publically available.

By connecting to a prospective employee through social networking sites, over-the-shoulder surfing while a prospective employee explores their social networking profile, or requiring an employee to change their privacy settings, an employer does not break the social networking law.¹¹¹ Despite not violating the letter of the Maryland social networking law, these go-arounds still conflict with the intent of the law. Through their online connection with the employee, the employer is able to view the information that the Maryland social networking law fights to protect.¹¹² Additionally, confusion in Maryland courts may ensue because even though employers are prohibited from asking for an employee's login or password to their

108. See *infra* Part V.A.

109. An employee may be able to argue that the request to connect online constitutes an invasion of privacy, but this claim may be made more difficult by the fact that the employee is presumed to have consented to the online connection. See Katherine A. Peebles, *Negligent Hiring and the Information Age: How State Legislatures Can Save Employers From Inevitable Liability*, 53 WM. & MARY L. REV. 1397, 1418 (2012) (noting that "consent is an absolute defense to intrusion upon seclusion.").

110. See Scott W. Pink, Jim Halpert & Russell H. Gardner, *Maryland's Employee Social Media Privacy Law: Five Exceptions, Five Ways Employers Can Prepare*, DLA PIPER (June 18, 2013), <http://www.dlapiper.com/maryland-restricts-employers-ability-to-access-employee-social-media/>.

111. None of these acts are prohibited by Maryland's social networking law. See MD. CODE ANN., LAB. & EMPL. § 3-712(b)(1) (West 2013).

112. Privacy violations may be limited if the employee has privacy settings enabled on their social networking account. Privacy settings differ from website to website as well as between users. However, Maryland's social networking law does not prevent an employer from asking or demanding that an employee not place the employer behind an online privacy wall.

social networking accounts, employers may still be obligated to view the same information if it is easily accessible to them.¹¹³

C. Lack of Penalties

Maryland's social networking law clearly prohibits employers from asking employees to divulge their username and passwords to social networking sites.¹¹⁴ However, there is no stated penalty for violating the law.¹¹⁵ Instead, the law authorizes the Maryland Attorney General to bring an action for appropriate relief.¹¹⁶ In an article examining California's social networking law, which similarly does not have any enforcement provisions, a writer for the Society for Human Resource Management states that "[e]mployer violations of this law could conceivably form the basis for an employee's wrongful termination action."¹¹⁷ In Maryland, employees have the ability to sue for wrongful termination when "the public policy allegedly contravened by the employer is 'sufficiently clear.'"¹¹⁸ In *Bleich v. Florence Crittenton Servs. of Baltimore, Inc.*, the Maryland Court of Special Appeals stated that "[l]egislative enactments, prior judicial decisions, [and] administrative regulations" are "the chief sources of public policy."¹¹⁹ Therefore, it is very likely that an employee would have the ability to sue an employer for wrongful termination by citing the Maryland social networking law. However, it is not clear what penalties such an employer would face.

D. Non-Applicability to Accounts Using Work Email

As the law firm DLA Piper notes in an article titled "Maryland's Employee Social Media Privacy Law: Five Exceptions, Five Ways Employers Can Prepare," employees may be entitled to no protection for certain accounts under Maryland's social networking law.¹²⁰ This is because Maryland's social networking law only

113. This information includes any detrimental information that one may easily find through online search engines such as Google. In instances in which the employer can easily obtain information about the employee by "friending" them on Facebook or "linking" to them on LinkedIn, an employer may violate due diligence in hiring by failing to take these actions. See *supra* Part V.A. However, it is unlikely that employers would be legally obligated to conduct over-the-shoulder reviewing of an employee's social networking profile or ask an employee to change their privacy settings as such actions would be highly intrusive.

114. See LAB. & EMPL. § 3-712(b)(1).

115. Note that there are no penalties listed in LAB. & EMPL. § 3-712 for violating the law's provisions. *Id.*

116. See LAB. & EMPL. § 3-712(f)(2).

117. Stuart Tochner, *Calif.: New Law Restricts Employer Access to Employee Social Media Accounts*, SOCIETY FOR HUMAN RESOURCE MANAGEMENT (Oct. 23, 2012), <http://www.shrm.org/LegalIssues/StateandLocalResources/Pages/Calif-Employee-Social-Media-Accounts.aspx>.

118. *Parks v. Alparma, Inc.*, 421 Md. 59, 74, 25 A.3d 200, 209 (2011).

119. 98 Md.App. 123, 134, 632 A.2d 463, 468 (quoting *Lee v. Denro*, 91 Md.App. 822, 830, 605 A.2d 1017, 1021 (1992)) (internal quotation marks omitted).

120. *Pink, Halpert & Gardner*, *supra* note 110.

applies to a “personal account or service.”¹²¹ Additionally, the law specifies that: “[a]n employer may require an employee to disclose any user name, password, or other means for accessing nonpersonal accounts or services that provide access to the employer’s internal computer or information systems.”¹²² Maryland’s social networking law fails to define the difference between a “personal” account and a “nonpersonal” account. DLA Piper, recognizing this ambiguity, suggests that a personal account is:

*limited to accounts that an employee sets up for his or her personal use unrelated to their work . . . [and] . . . may well not apply to non-personal accounts, such as a Twitter account an employee sets up in connection with work using his or her work email address, or a LinkedIn account an employee sets up under his or her corporate email address to populate contacts related to his or her work.*¹²³

Although such an expansive definition may not accord with the spirit of Maryland’s social networking law, the fact that a prominent law firm interprets the law in this manner reveals a troubling ambiguity. Employees may mistakenly believe that their usernames and passwords to accounts that they consider “personal” are protected under Maryland’s social networking law. However, such accounts may be viewed under the law as “nonpersonal” accounts. The failure of Maryland’s social networking law to define “personal” and “nonpersonal” is an oversight that needs to be corrected.

E. Universities and Social Networking: The Next Battleground?

One of the times in which people are forced to connect online with their supervisors is not in a work environment, but rather the college environment. Students and universities are similarly situated to employees and employers, respectively. Universities must make decisions on whether to accept and retain students, similar to how employers must determine whether to hire and retain employees. Employees and students are both at a steep disadvantage in their relationships with employers and universities, respectively.¹²⁴ The absence of any

121. MD. CODE ANN., LAB. & EMPL. § 3-712(b)(1) (West 2013).

122. LAB. & EMPL. § 3-712(b)(2).

123. Pink, Halpert & Gardner, *supra* note 110. See generally David Coursey, *Who Owns Your LinkedIn Contacts?*, FORBES (Nov. 3, 2011), <http://www.forbes.com/sites/davidcoursey/2011/11/03/who-owns-your-linkedin-contacts/>.

124. Employees are at a power disadvantage because they rely on their employers for employment. The high national unemployment rate provides additional power to employers when choosing prospective employees. Likewise, universities that are selective in who they admit have the power to shape an applicant’s future depending on whether or not the university admits them. Once the student is admitted, the university has the

language in Maryland's social networking law protecting students is a deliberate omission by Maryland's social networking law that should be corrected.¹²⁵

1. Educational Institutions' Social Networking Monitoring

Schools such as the University of Kentucky and the University of Louisville require athletes to consent to monitoring software on their social networking accounts as a precondition of participating in university athletics.¹²⁶ The monitoring software flags hundreds of words that relate to drugs, sex, or alcohol as well as words such as sports agents' names.¹²⁷ The software that the universities use scans athletes' "posts, tweets, comments, and any other information submitted online."¹²⁸ Any flagged information generates an email that is sent to the athlete's coach.¹²⁹ Because university judicial proceedings are private, it is unclear what, if any consequences student athletes have faced from their online postings.¹³⁰ Nevertheless, with the release of over 1,500 pages of posts under a Freedom of Information Act request from the University of Kentucky, it is clear that the monitoring software is often being put to use.¹³¹ ACLU Attorney William Sharp states that "[w]hen students are forced, as a condition of receiving a scholarship, to grant government officials access to all of their social networking accounts and then are subject to punishment for engaging in lawful speech that the university simply doesn't like, we believe public universities cross the line."¹³²

Despite increasing public recognition of universities' monitoring of the social networking accounts of their athletes, it is highly unlikely that universities will move away from these monitoring programs as the decision of universities to use social networking monitoring software to monitor athletes is implicitly supported by the actions of the National Collegiate Athletic Association (NCAA), the organization

power to force them to adhere to their judicial guidelines, which may include a social networking policy, as part of their attendance at the university.

125. See *infra* Part.V.E.2, regarding a Maryland bill protecting the social media of students, which failed to pass.

126. Mark Boxley, *University of Kentucky, Louisville monitor athletes' tweets*, USA TODAY (Aug. 20, 2012), <http://usatoday30.usatoday.com/sports/college/story/2012-08-20/University-of-Kentucky-and-University-of-Louisville-student-athletes-monitored-on-Twitter/57165704/1>.

127. *Id.*

128. *Id.*

129. *Id.*

130. Boxley, *supra* note 126.

131. *Id.* The Kentucky ALCU, a different branch of the national ACLU organization whose Maryland chapter led the push for Maryland's social networking law, is firmly against such monitoring. *Id.*

132. *Id.*

that controls college athletics.¹³³ In March 2012, the NCAA imposed harsh punishment on the University of North Carolina, Chapel Hill by banning the university from postseason play the following fall and taking away fifteen athletic scholarships over three years.¹³⁴ The NCAA took those actions after finding that the athletic program committed academic fraud, provided illicit payments to athletes, and committed other unethical conduct.¹³⁵ In their report, the NCAA stated that if the university had monitored their athletes' social networking sites, they would have discovered some of the violations earlier.¹³⁶ The NCAA's report also stated that "[w]hile we do not impose an absolute duty upon member institutions to regularly monitor such sites, the duty to do so may arise as part of an institution's heightened awareness when it has or should have a reasonable suspicion of rules violations."¹³⁷ With the NCAA's implicit endorsement of the monitoring of athletes' social networking pages and universities at risk of serious consequences for failing to find offensive or illegal posts, it is likely that universities will increasingly use monitoring technology.

It is not only students at the university-level who are subject to monitoring software. Glendale, California, a school district in suburban Los Angeles, is paying a contractor to monitor the social networking websites of 14,000 students in the district's middle and high schools.¹³⁸ The software works similarly to the software monitoring university athletes except that it also monitors whether students are discussing skipping class as well as their use of smartphones during school.¹³⁹ The software utilized by the contractor does not require students to reveal their usernames and passwords,¹⁴⁰ but there is no protection for students if the school system chose to require students to provide such information as a condition of their enrollment. While monitoring programs of younger students are not currently in widespread use, such programs may be viewed as a method to combat the online

133. See Kelly Whiteside, *North Carolina, NCAA address monitoring social media*, USA TODAY (Mar. 12, 2012), <http://content.usatoday.com/communities/campusrivalry/post/2012/03/north-carolina-ncaa-address-monitoring-social-media/1#.UQ2WO6WClwF>.

134. Doug Lederman, *Another NCAA Power Punished*, INSIDE HIGHER ED (Mar. 13, 2012), <http://www.insidehighered.com/news/2012/03/13/unc-becomes-latest-ncaa-power-face-association-punishment>.

135. *Id.*

136. See Whiteside, *supra* note 133.

137. *Id.* The NCAA later pulled back slightly from their comments by stating that "[t]he NCAA was not going to impose a blanket duty on members to monitor social-networking websites . . ." Michael Felder, *North Carolina Football: Case Sheds Light on NCAA Social Media Policy*, BLEACHER REPORT (Mar. 13, 2012), <http://bleacherreport.com/articles/1102257-college-football-2012-unc-case-sheds-light-on-ncaa-social-media-policy>.

138. Michael Martinez, *California school district hires firm to monitor students' social media*, CNN, <http://www.cnn.com/2013/09/14/us/california-schools-monitor-social-media/> (last updated Sept. 18, 2013).

139. *Id.*

140. *Id.*

problem of cyberbullying. The Florida School Boards Association, situated in a state with 2.8 million students, states that it expects the popularity of such monitoring programs to increase,¹⁴¹ possibly as a response to tragedies such as the death of Rebecca Sedwick, a student, through cyberbullying.¹⁴²

2. Maryland's Social Networking Law's Impact on Universities' Monitoring of Students' Social Networking Accounts

Maryland's social networking law does not protect students whose university requires them to consent to monitoring of their social networking account. Maryland's social networking law specifically prohibits an employer from requesting or requiring access to the social networking account of an employee or applicant.¹⁴³ Therefore, a straightforward reading of the law indicates that the social networking law only applies to the employer-employee relationship. Legislative history provides further evidence that the Maryland social networking law was not meant to address the monitoring of students' social networking accounts. Bills were introduced into the Maryland legislature specifically addressing that issue at the same time the Maryland social networking law was being considered.¹⁴⁴ Senate Bill 434, the "Institutions of Postsecondary Education - Electronic Account, Service, and Communications Device Privacy Protection Act", prohibited any university from requiring a student to disclose their social networking account information.¹⁴⁵ House Bill 746, the cross-filed bill with the Maryland House of Delegates, prohibited universities from installing on communication devices "software that monitors or tracks electronic content."¹⁴⁶ Maryland's social networking law, which passed the Maryland Senate unanimously on March 14, 2012, explicitly rejected that prohibition by striking out that language, originally included in the bill, by amendment.¹⁴⁷ Neither Senate Bill 434 nor House Bill 746 became law as a result of the "logjam" created by Maryland legislature's inability to pass a budget.¹⁴⁸

141. *Should schools monitor students' social media?*, FOX 13: TAMPA BAY (Oct. 16, 2013, 4:57 PM), <http://www.myfoxtampabay.com/story/23710238/2013/10/16/should-schools-monitor-students-social-media>.

142. *See generally* Emily Bazelon, *Bullies Taunted Rebecca Ann Sedwick with Texts Like "Can u Die Please?" And Then She Did.*, SLATE (Sept. 18, 2013), http://www.slate.com/blogs/xx_factor/2013/09/18/rebecca_ann_sedwick_suicide_lessons_for_parents_in_the_scary_age_of_cyberbullying.html.

143. MD. CODE ANN., LAB. & EMPL. § 3-712(b)(1) (West 2013).

144. *See* S.B. 434, 2012 Leg., 430th Sess. (Md. 2012); H.D. 746, 2012 Leg., 430th Sess. (Md. 2012).

145. *See* Md. S.B. 434(B)(1).

146. Md. H.D. 746(B)(1)(III).

147. *See* S.B. 434, 2012 Leg., 430th Sess. (Third Reading) (Md. 2012).

148. Shear, *supra* note 75.

F. An Improved Social Networking Law

Maryland's social networking law has many flaws that decrease the law's effectiveness. These flaws include a lack of clarity on how the law affects an employer's duty of due diligence in hiring its workforce; various loopholes that enable employers to view the exact type of information that the law was trying to prevent employers from viewing; no penalties for a violation of the law; ambiguity regarding what constitutes a "personal account;" and a total lack of protections for students' social networking accounts. Failure to correct these issues could lead individual judges to interpret the law on a piecemeal basis. Instead, similar to how Maryland legislators amended Maryland's social networking law in July 2013 to include enforcement provisions,¹⁴⁹ legislators should once again amend the law to fix its many loopholes and ambiguities.

1. Clarify the Requirements of Due Diligence

To eliminate any confusion regarding an employer's responsibility of due diligence, Maryland may want to follow the lead of states like Michigan. Michigan's social networking law states that it explicitly does not prohibit viewing any information publically available and that it does not create a duty to "search or monitor the activity of a personal internet account."¹⁵⁰ This unequivocal clarification eliminates the guesswork of whether employers may still have a duty of due diligence regarding an applicant's or employee's social networking account. By including a similar provision in its social networking law, Maryland would ensure that employers are aware that they are allowed to conduct public online searches, but are under no duty to search for information on an individual's social networking page.¹⁵¹

2. Prioritize the Protection of Private Information

Maryland's social networking law needs to be rewritten to protect the private information that a person places on their social networking page as it is insufficient to only protect a person's username and password. States, including California, Washington, and Michigan, have social networking laws that focus on the protection of private information. For example, California's social networking law specifies that employers cannot require employees to provide them with "any

149. MD. CODE ANN., LAB. & EMPL. § 3-712(f) (West 2013).

150. H.B. 5523, 96th Leg., Reg. Sess. (Mich. 2012).

151. A policy that specifies that employers are under no duty to search the private social networking websites of employees and prospective employees will be beneficial to employers and employees alike. However, an important public policy question that remains is what degree an employer should concern themselves with the online lives of its employees and prospective employees?

personal social media.”¹⁵² Michigan’s social networking law similarly prohibits employers from asking an applicant or employee to “grant access to, allow observation of, or disclose information” regarding a person’s social networking account.¹⁵³ By prohibiting access to the content of the account rather than just the username and password to the account, employers are prohibited from requiring employees and applicants to “friend” them or connect with them through LinkedIn. Additionally, employers are prohibited from shoulder-surfing to view the content of a personal social networking pages of an employee or applicant. Washington’s social networking law, which took effect in July 2013, explicitly prohibits an employer from shoulder-surfing, requiring employees to connect online, and demanding that employees change their privacy settings.¹⁵⁴ Lawmakers in Maryland may want to consider amending Maryland’s social networking law to provide similar protections.

3. Mandate Effective Penalties

Effective penalties would deter employers from asking employees for their social networking username and password by putting employers on notice that they will face punishment for their illegal practices. The possibility that the only time an employer would encounter Maryland’s social networking law is after an employee has been terminated is insufficient. The option of a wrongful termination action would provide little help to an applicant who was not hired after refusing to provide their social networking username and password.¹⁵⁵ Washington’s social networking law could provide a model for Maryland. The law contains language that states that “[a]n employee or applicant aggrieved by a violation of . . . this act may bring a civil action.”¹⁵⁶ Washington’s social networking law also enables a court to order injunctive as well as equitable relief, assess a \$500 penalty, and allows for the recovery of attorney’s fees.¹⁵⁷ By amending Maryland’s social networking law to include language that authorizes specific monetary penalties, lawmakers will ensure that the law sufficiently deters illegal behavior.

152. 2012 Cal. Legis. Serv. Ch. 618 (A.B. 1844) (West).

153. Mich. H.B. 5523.

154. See WASH. REV. CODE ANN. §49.44.0003 (West 2013). See also Victor Li, *Washington State Turns Up the Privacy for Social Media*, LAW TECHNOLOGY NEWS (July 30, 2013), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202613118396&Washington_State_Turns_Up_the_Privacy_for_Social_Media&slretur n=20130828182654.

155. Moreover, an employee may never be certain of the reasons for which they were not hired. As one employment website stated, these types of cases are “hard to know – and harder to prove.” *Lawsuits Based on the Hiring Process*, NOLO, <http://www.nolo.com/legal-encyclopedia/lawsuits-based-the-hiring-process.html> (last visited Nov. 10, 2013).

156. WASH. REV. CODE ANN. §49.44.0003 (West 2013).

157. *Id.*

4. *Pass Legislation Protecting Students*

To properly protect students and athletes, Maryland should follow the lead of Delaware, which enacted a law solely targeted at academic institutions. The law in Delaware prohibits both public and nonpublic academic institutions from requesting the username of a student or applicant.¹⁵⁸ Additionally, the law in Delaware forbids academic institutions from requiring a student or applicant to install monitoring software on their account.¹⁵⁹ The state also addresses some of the previously mentioned loopholes of Maryland's social networking law by prohibiting such actions as shoulder-surfing and requiring a person to connect with the academic institution on the social networking website.¹⁶⁰ Maryland legislators should reintroduce and pass Senate Bill 434, which prohibited universities from requiring students to disclose their social networking usernames and passwords.

VI. CONCLUSION

As social networking's popularity shows no signs of slowing down,¹⁶¹ particularly with the ability for people to easily access their social networking accounts on their phones,¹⁶² the online "private" lives of job applicants and employees will increasingly cause friction with employers. Maryland's social networking law is a strong first step in ensuring that job applicants and employees are able to keep their private information on their social networking accounts from interested employers. It is an obvious improvement over the legal void that existed before the law came into effect. While some of the solutions for these issues are straightforward, such as reintroducing and passing Senate Bill 434, which provides comprehensive protections for students, other solutions such as determining what financial penalty will sufficiently deter employers from illegal acts will be more complicated. If Maryland's social networking law is not clarified or reinforced, it will fail to provide the protection to employers and employees that the law's drafters originally intended.

158. H.B. 309, 146th Gen. Assemb., Reg. Sess. (Del. 2012).

159. *Id.*

160. *Id.* Delaware also prohibits academic institutions from accessing the social networking profile or a student or applicant indirectly through a third-person. *Id.*

161. See Donna Tam, *Facebook by the Numbers: 1.06 billion monthly active users*, CNET (Jan. 30, 2013), http://news.cnet.com/8301-1023_3-57566550-93/facebook-by-the-numbers-1.06-billion-monthly-active-users/.

162. *Id.*