

6-1-2015

# From Due Diligence To Discrimination: Employer Use of Social Media Vetting In The Hiring Process And Potential Liabilities

Jennifer Delarosa

*J.D. Candidate, Loyola Law School, Los Angeles, 2016*

---

## Recommended Citation

Jennifer Delarosa, *From Due Diligence To Discrimination: Employer Use of Social Media Vetting In The Hiring Process And Potential Liabilities*, 35 Loy. L.A. Ent. L. Rev. 249 (2015).

Available at: <http://digitalcommons.lmu.edu/elr/vol35/iss3/1>

This Notes and Comments is brought to you for free and open access by the Law Reviews at Digital Commons @ Loyola Marymount University and Loyola Law School. It has been accepted for inclusion in Loyola of Los Angeles Entertainment Law Review by an authorized administrator of Digital Commons@Loyola Marymount University and Loyola Law School. For more information, please contact [digitalcommons@lmu.edu](mailto:digitalcommons@lmu.edu).

# **FROM DUE DILIGENCE TO DISCRIMINATION: EMPLOYER USE OF SOCIAL MEDIA VETTING IN THE HIRING PROCESS AND POTENTIAL LIABILITIES**

*Jennifer Delarosa\**

This Note analyzes the regulatory and legal issues potentially triggered by an employer's screening and use of an applicant's social media profile(s) in the hiring process. The Note proceeds in three parts. Part I provides background information, including a history of the rise and use of social media in the hiring process, current various state and federal legislative measures designed to protect applicants' online privacy, and the reasoning behind such legislation. Part II discusses the potential discrimination and other labor and employment-related lawsuits to which employers may be exposed by using online information in hiring practices. It is important to mention that the Note does not focus on issues of privacy in pre-employment screening. Instead, the Note is concerned with discrimination claims in pre-employment screening; specifically, claims under Title VII of the Civil Rights Act, the Age Discrimination in Employment Act, and some state laws prohibiting "lifestyle discrimination." After addressing the distinct legal issues triggered by the use of social media in hiring decisions, Part III analyzes pending legislation and its inefficiencies and considers the significance of why employers should self-regulate. The Note then concludes by proposing best practices and guidelines for the development of a social media screening policy that reduces an employer's risk of litigation surrounding pre-employment social media screening.

---

\*J.D. Candidate, Loyola Law School, Los Angeles, 2016; B.A., University of California, Berkeley, 2013. Thank you to Loyola Law School Professor Carlos Berdejó and to the editors of the *Loyola of Los Angeles Entertainment Law Review* for their insight and thoughtful review.

Right before we interviewed a recent college graduate, we discovered that one of his interests listed on his [social networking] profile is ‘Smokin’ blunts with the homies and bustin’ caps in whitey’ and one of his favorite quotes is ‘Beware of big butts and a smile.’ Our ‘first impression’ of our candidate was officially tainted, and he had little hope of regaining a professional image in our eyes. He was not hired.

—Brad Karsh, President, JobBound<sup>1</sup>

## I. INTRODUCTION

For better or worse, the Internet has made the availability and collection of information easier than ever before.<sup>2</sup> In particular, social networking sites provide a platform for a user to upload content, connect with others, and view information.<sup>3</sup> Indeed, this virtual platform works quite literally as a “platform,” showcasing material by providing it to a mass audience.<sup>4</sup> Consequently, with the boundless reach of the Internet—and thus, the boundless audience—employers are using social networking sites to screen prospective employees.<sup>5</sup>

Not surprisingly, pre-employment screening is not new. Labor

---

1. *MySpace Is Public Space When It Comes to Job Search*, COLLEGEGRAD.COM (July 26, 2006), <https://collegegrad.com/press/myspace>.

2. See, e.g., David H. Autor, *Wiring the Labor Market*, 15 J. ECON. PERSP. 25, 26 (2001) (discussing the advantages of internet job boards).

3. See *Characteristics of Web 2.0 Technology*, TECHPLUTO (Nov. 28, 2008), <http://www.techpluto.com/web-20-services/>.

4. *Id.*

5. See, e.g., Aubrey Wieber, *More Employers Using Social Media to Screen Applicants*, POST REGISTER (June 25, 2014, 4:00 AM), <http://www.postregister.com/articles/featured-news/2014/06/25/more-employers-using-social-media-screen-applicants>; see Erica Swallow, *How Recruiters Use Social Networks to Screen Candidates*, MASHABLE (Oct. 23, 2011), <http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/>.

market search theory predicts that when an employer and employee can more efficiently make a high-quality “match” through pre-employment screening, output, worker earnings, and business profits all rise.<sup>6</sup> With this result in mind, employers often seek as much information as possible about job applicants to ensure the best match between an applicant and the employer’s organization.<sup>7</sup> In order to obtain such information, employers have utilized a vast number of information-gathering techniques, depending largely on the position to be filled.<sup>8</sup> Historically, pre-employment screening techniques for gathering information about applicants have included written applications, questionnaires, interviews, references (personal references and previous employment references), background checks, credit checks, and a variety of pre-employment tests, such as polygraph, psychological, medical, drug, and ability tests.<sup>9</sup> Employers are generally permitted to investigate applicants; however, several legal concerns arising from online investigations have become a major focus of recent legislation and litigation.<sup>10</sup> Between the risks of negligent hiring and online information gathering, what’s an employer to do?

This Note analyzes the regulatory and legal issues potentially triggered by an employer’s screening and use of an applicant’s social media profile in the hiring process and proceeds in three parts. Part II provides background information, including a history of the rise and use of social

---

6. See Autor, *supra* note 2, at 27.

7. See Stephen F. Befort, *Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place*, 14 HOFSTRA LAB. L.J. 365, 367 (1997).

8. *Id.* at 368.

9. See Rochelle B. Ecker, Comment, *To Catch a Thief: The Private Employer’s Guide to Getting and Keeping an Honest Employee*, 63 UMKC L. REV. 251, 255–61 (1994) (outlining traditional methods of pre-employment screening).

10. See *Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure, and Social*, PRIVACY RIGHTS CLEARINGHOUSE, <https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social> (June 2010) (“The Fair Credit Reporting Act (FCRA) is a law that not only regulates credit reports but also sets national standards for employment screening and background checks. In effect, it sets limits on what information employers can get from background checks and how they can use that information . . . . However, the FCRA only applies to employers using third-party screening companies. Information that an employer gathers independently, including from informal Internet searches, is not covered by the FCRA.”); see generally, e.g., *Gaskell v. Univ. of Ky.*, No. 09-244-KSF, 2010 U.S. Dist. LEXIS 124572 (E.D. Ky. Nov. 23, 2010) (discussing the harm that can arise when prospective employers have access to personal social media accounts of applicants and base hiring decisions on information gathered from such sources).

media in the hiring process, several current state and federal legislative measures designed to protect applicants' online privacy, and the reasoning behind such legislation. Part III discusses the potential discrimination and other labor and employment-related lawsuits to which employers may be exposed to by using online information in hiring practices. After addressing the distinct legal issues triggered by the use of social media in hiring decisions, Part IV analyzes pending legislation and its inefficiencies and considers the significance of why employers should self-regulate. The Note then concludes by proposing best practices and guidelines for developing a social media screening policy that reduces an employer's risk of litigation surrounding pre-employment social media screening.

## II. BACKGROUND

### A. *The Rise of Social Media*

For the purposes of this Note, social networking sites are defined as “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”<sup>11</sup> The key to a social networking site is that individuals have public and visible social networking profiles and information that is shared with that individual's “Friends,” or users of that social network identified as having a relationship with that individual.<sup>12</sup> “Friends” can be identified with different labels depending on the social networking site.<sup>13</sup> Generally, this Note combines these various social networking sites under the term “social media.”

Given the dozens of social media platforms available, each can be categorized in terms of the function that it serves.<sup>14</sup> Social media that “disseminates writings and information on an ongoing or real time basis”

---

11. Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2008), available at <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full> (follow “Get PDF (217K)” hyperlink).

12. *Id.* at 213.

13. *Id.*

14. Carolyn Elefant, *The “Power” of Social Media: Legal Issues & Best Practices for Utilities Engaging Social Media*, 32 ENERGY L.J. 1, 4 (2011).

may be categorized as communication.<sup>15</sup> For example, blogs and Twitter accounts fall under communication.<sup>16</sup> Directories, such as LinkedIn, provide a “resume-type listing with ratings by clients and colleagues.”<sup>17</sup> In contrast to directories, community and rating sites such as Facebook, Google+, and Yelp, consist of “collegial or less formal interaction [within a] closed site.”<sup>18</sup> Lastly, archiving and sharing sites, such as YouTube, Flickr, and Scribd, “store, share, and redistribute video, slides and documents with opportunity for feedback.”<sup>19</sup> While social media has evolved to perform various functions, this technology ultimately facilitates interactive information, user-created content, and collaboration.<sup>20</sup>

The first known and recognized social networking website launched in 1997 and was named “SixDegrees.”<sup>21</sup> SixDegrees allowed users to “create profiles, list their Friends and . . . surf the Friends lists.”<sup>22</sup> SixDegrees aimed to connect people online by allowing individuals to send messages to one another.<sup>23</sup> Several more social networking sites launched over the next few years. This burst started in 2003 with the creations of LinkedIn and MySpace.<sup>24</sup> Facebook began the following year as a Harvard student-only social network site.<sup>25</sup> Facebook then opened up to students from other universities in 2005, just as YouTube launched its video-based

---

15. *Id.*

16. *Id.*

17. *Id.*

18. *Id.* at 5.

19. *Id.*

20. See generally *Characteristics of Web 2.0 Technology*, TECHPLUTO (Nov. 28, 2008), <http://www.techpluto.com/web-20-services/> (describing the characteristics of Web 2.0 Technology).

21. Boyd & Ellison, *supra* note 11, at 214.

22. *Id.*

23. *Id.*

24. *Id.* at 216.

25. *Id.* at 218.

site.<sup>26</sup> While Facebook expanded to allow access to nearly anyone with an email address in 2006, Twitter also arrived onto the worldwide social network scene.<sup>27</sup> In August 2010, for the first time, Facebook surpassed Google as the number one site where Internet users spend the majority of their online time.<sup>28</sup> Thus, if an employer seeks to gather information about a job candidate, one's social media presence is virtually guaranteed for perusal.

Employers are catching on to the readily accessible information on the Internet and are increasingly using candidates' social media sites in order to assess a candidate during recruitment and hiring.<sup>29</sup> Some employers claim to look for whether the candidate fits the company's corporate culture, presents him or herself in a professional manner, or meets certain job qualifications.<sup>30</sup> Social media can also serve as a reference tool to learn about a candidate's work style, whether a candidate will incur serious legal liabilities, or to vet a candidate's ability to protect proprietary information and comply with federal regulations.<sup>31</sup> Although the studies that assess the percentage of employers that use social networks to screen candidates vary widely in their conclusions, the most conservative studies estimate that approximately one to two fifths of employers are searching job applicants on Facebook, LinkedIn, or any number of other

---

26. *Id.*; Sarah Kehaulani Goo, *Ready For Its Close-Up*, WASH. POST (Oct. 7, 2006), <http://www.washingtonpost.com/wp-dyn/content/article/2006/10/06/AR2006100600660.html>.

27. Boyd & Ellison, *supra* note 11, at 218; Michael Arrington, *Odeo Releases Twtr*, TECHCRUNCH (July 15, 2006), <http://techcrunch.com/2006/07/15/is-twtr-interesting/>.

28. Nick O'Neill, *Facebook Surpasses Google in "Time Spent" On Site Domestically*, ADWEEK (Sept. 10, 2010, 11:16 AM), [http://allfacebook.com/facebook-surpasses-google-in-time-spent-on-site-domestically\\_b18670](http://allfacebook.com/facebook-surpasses-google-in-time-spent-on-site-domestically_b18670).

29. Laxmikant Manroop & Julia Richardson, *Using Social Media for Job Search: Evidence from Generation Y Job Seekers*, in 12 ADVANCED SERIES IN MANAGEMENT: SOCIAL MEDIA IN HUMAN RESOURCES MANAGEMENT 167, 168 (Tanya Bondarouk & Miguel R. Olivas-Juján eds., 2013) (reporting that, according to a 2011 Jobvite recruitment survey, eighty-nine percent of the 800 companies surveyed indicated an intent to recruit through social media, compared to eighty-three percent the year prior).

30. *The Role of Social Media in Pre-Employment Candidate Screening- Statistics and Trends*, GO-GULF (Feb. 22, 2014), <http://www.go-gulf.com/blog/social-media-pre-employment-screening/>.

31. *See generally id.* (realizing that a candidate's social media activities present an accurate picture of who the candidate is).

search engines and social networks.<sup>32</sup> Some estimate that the number is much higher—claiming that as many as ninety percent of employers are using social networks at some point during the hiring process.<sup>33</sup> Ultimately, the practice of social media vetting can afford the employer access to information about the candidate that they might not otherwise find in the candidate’s application.

### *B. Controversies Leading to Social Media Privacy Legislation*

Several publicized controversies prompted state legislatures and Congress to consider and enact laws restricting employers’ access to social media login information. The issue first gained traction in Maryland in 2011.<sup>34</sup> There, a former officer with the Maryland Department of Public Safety and Correctional Services complained about being asked to provide his Facebook password during a recertification interview.<sup>35</sup> The Department began asking prospective employees for Facebook login information a year prior, as part of a background check to screen

---

32. See Aubrey Wieber, *More Employers Using Social Media to Screen Applicants*, POST REGISTER (June 25, 2014, 4:00 AM), <http://www.postregister.com/articles/featured-news/2014/06/25/more-employers-using-social-media-screen-applicants> (reporting that, “according to the Society for Human Resource Management, twenty percent of employers screen applicants by Googling them and scanning their social media profiles”); *Number of Employers Passing on Applicants Due to Social Media Posts Continues to Rise*, CAREERBUILDER (June 26, 2014), <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014> (reporting that, according to a new survey by CareerBuilder.com, forty percent of employers research job candidates on social media).

33. See Erica Swallow, *How Recruiters Use Social Networks to Screen Candidates*, MASHABLE (Oct. 23, 2011), <http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/> (reporting that, according to a Reppler survey, “90 percent of recruiters and hiring managers have visited a potential candidate’s profile on a social network as part of the screening process”); Dan Schawbel, *How Recruiters Use Social Networks to Make Hiring Decisions Now*, TIME (July 9, 2012), <http://business.time.com/2012/07/09/how-recruiters-use-social-networks-to-make-hiring-decisions-now/> (reporting that, according to a new survey by Jobvite, ninety-two percent of employers use or plan to use social networks for recruiting).

34. Philip Gordon, Steven Kaplan, & Ashley Sims, *Legislation Roundup: Maryland “Facebook Law” Raises New Obstacles for Employers and Other Significant Maryland Developments*, LITTLER (Apr. 17, 2012), <http://www.littler.com/publication-press/publication/legislation-roundup-maryland-facebook-law-raises-new-obstacles-employe>.

35. Catherine Ho, *Md. Employers Cannot Collect Facebook Passwords*, WASH. POST (Apr. 15, 2012), [http://www.washingtonpost.com/business/capitalbusiness/md-employers-cannot-collect-facebook-passwords/2012/04/13/gIQAzwQtJT\\_story.html](http://www.washingtonpost.com/business/capitalbusiness/md-employers-cannot-collect-facebook-passwords/2012/04/13/gIQAzwQtJT_story.html).



employees for gang affiliations.<sup>36</sup> The state's American Civil Liberties Union ("ACLU") chapter took a stance against this new practice, and in response to public outcry, the Department temporarily suspended and then revised its policy to allow applicants to "voluntarily participate" in a review of their social media accounts.<sup>37</sup> Subsequently, in May 2012, Maryland Governor Martin O'Malley signed into law the User Name and Password Privacy Protection Act, proposed and passed by the Maryland legislature.<sup>38</sup> This law was the first of its kind and marked the beginning of a nationwide trend of social media privacy protection.<sup>39</sup>

Another controversy surfaced in 2009 when the city government of Bozeman, Montana, instructed applicants to divulge their usernames and passwords for social media sites, including Facebook, Google, Yahoo, YouTube, and MySpace.<sup>40</sup> Although the city argued that it only used the information to verify application information, nationwide criticism and outrage prompted the city to cease its hiring practice.<sup>41</sup>

A third controversy occurred in Minnesota when a young female student claimed her public school brought her into a room with a police officer present, and forced her to provide her Facebook login information and email accounts because of allegations that she had online conversations about sex with another student.<sup>42</sup> The ACLU of Minnesota filed a lawsuit

---

36. *Id.*

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

38. Gordon *et al.*, *supra* note 34; see Melissa Cortez Goemann, *Maryland Passes Nation's First Social Media Privacy Protection Bill*, ACLU (May 4, 2012, 4:30 PM), <https://www.aclu.org/blog/technology-and-liberty/maryland-passes-nations-first-social-media-privacy-protection-bill>.

39. Goemann, *supra* note 38.

40. Declan McCullagh, *Want a Job? Give Bozeman Your Facebook, Google Passwords*, CNET (June 18, 2009, 4:52 PM), <http://www.cnet.com/news/want-a-job-give-bozeman-your-facebook-google-passwords/>.

41. Matt Gouras, *Montana City Asks Job Applicants for Facebook Passwords*, HUFFINGTON POST, [http://www.huffingtonpost.com/2009/06/19/montana-city-asks-job-app\\_n\\_218152.html](http://www.huffingtonpost.com/2009/06/19/montana-city-asks-job-app_n_218152.html) (last updated May 25, 2011, 1:30 PM); see Ki Mae Heussner, *Montana City Asks Job Applicants for Online Passwords*, ABC NEWS (June 19, 2009), <http://abcnews.go.com/Technology/JobClub/story?id=7879939>.

42. *ACLU-MN Files Lawsuit Against Minnewaska Area Schools*, ACLU OF MINN. (Mar. 6, 2012), <http://www.aclu-mn.org/news/2012/03/06/aclu-mn-files-lawsuit-against-minnewaska>.

in 2012 against the Minnewaska Area Schools and the Pope County Sheriff's office for violating the student's constitutional rights.<sup>43</sup> Specifically, the ACLU-MN argued a violation of the student's First Amendment right to freedom of speech and Fourth Amendment right to be free from unreasonable searches and seizures.<sup>44</sup> Minnewaska Area Schools agreed to pay \$70,000 to settle the lawsuit in March 2014 and to "rewrite its policies to limit how intrusive the school can be when searching a student's emails and social media accounts created off school grounds."<sup>45</sup>

Each of the aforementioned controversies arose out of requirements by a government agency to disclose social media information. Despite the trend requiring more detailed and in-depth information for job applicants, these instances have led state legislators to believe that statutory protection is necessary.

### C. Laws Regulating Employers

#### 1. State Laws

In 2012, four states enacted legislation that prohibits employers from requesting an applicant to disclose a username or password for a social media account: California, Illinois, Maryland, and Michigan.<sup>46</sup> Ten other states proposed legislation in 2012: Delaware, Massachusetts, Minnesota, Missouri, New Jersey, New York, Ohio, Pennsylvania, South Carolina, and Washington.<sup>47</sup> In 2013, the enactment of employment-related social media password protection laws increased dramatically. An additional thirty-six states proposed laws in 2013.<sup>48</sup> Eight of these states passed their acts in

---

area-schools.

43. *Id.*

44. *Id.*

45. Curt Brown, *ACLU Wins Settlement for Sixth-Grader's Facebook Posting*, STAR TRIBUNE, <http://www.startribune.com/local/252263751.html> (last updated Mar. 25, 2014, 11:06 PM).

46. *Employer Access to Social Media Usernames and Passwords: 2012 Legislation*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 17, 2013), <http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx>.

47. *Id.*

48. *Id.*

2013: Arkansas, Colorado, Illinois, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and Washington.<sup>49</sup> Five other states—Indiana, New York, Oklahoma, Tennessee, and Wyoming—proposed legislation the following year.<sup>50</sup> As of writing this Note, Louisiana, Maine, New Hampshire, Oklahoma, Rhode Island, Tennessee, and Wisconsin enacted legislation in 2014.<sup>51</sup> In sum, twenty-one states have enacted legislation regulating employer use of employees’ social media.

Vital to the scope of social media legislation is how a statute defines the term “employer.” Many employment statutes define “employer” generally as a person, individual, or entity engaged in a business, industry, profession, trade, or enterprise in the state or a unit of state or local government.<sup>52</sup> Uniquely, however, both the Colorado and New Jersey legislation specify that “employer” does not include the department of corrections, county corrections departments, or any state or local law enforcement agency.<sup>53</sup> New Mexico also excludes similar agencies through an exception.<sup>54</sup> In relation to this issue, the California State

---

49. Those states are: Arkansas, Colorado, Nevada, New Mexico, Oregon, Utah, Vermont, and Washington. *Id.*

50. *Id.*

51. *Id.*

52. *See, e.g.*, ARK. CODE ANN. § 11-2-124 (2013) (“‘Employer’ means a person or entity engaged in business, an industry, a profession, a trade or other enterprise in the state or a unit of state or local government, including without limitation an agent, representative, or designee of the employer . . . .”); MD. LAB. & EMPL. CODE ANN. § 3-712 (LexisNexis 2013) (“‘Employer’ means: 1. a person engaged in a business, an industry, a profession, a trade, or other enterprise in the State; or 2. a unit of State or local government”); MICH. COMP. LAWS SERV. § 37.272 (LexisNexis 2012) (“‘Employer’ means a person, including a unit or local government, engaged in a business, industry, profession, trade, or other enterprise in this state and includes an agent, representative, or designee of the employer.”).

53. COLO. REV. STAT. § 8-2-127 (2013) (“‘Employer’ means a person engaged in a business, industry, profession, trade, or other enterprise in the state or a unit of state or local government. ‘Employer’ includes an agent, a representative, or a designee of the employer. ‘Employer’ does not include the department of corrections, county corrections departments, or any state or local law enforcement agency.”); N.J. STAT. ANN. § 34:6B-5 (West 2014) (“‘Employer’ means an employer or employer’s agent, representative, or designee. The term ‘employer’ does not include the Department of Corrections, State Parole Board, county corrections departments, or any State or local law enforcement agency.”).

54. N.M. STAT. ANN. § 50-4-34 (2013) (“Nothing in this section shall apply to a federal, state or local law enforcement agency. Nothing in this section shall prohibit federal, state or local government agencies or departments from conducting background checks as required by law.”).

Assembly has introduced a bill that would amend existing law to prohibit both private and public employers from requesting an employee or applicant's social media login information, with the exception of law enforcement agencies.<sup>55</sup> The bill is currently awaiting a vote in the state Senate.<sup>56</sup>

## 2. Federal Laws

Congress has also proposed legislation of this kind. First introduced in April 2012, the Social Networking Online Protection Act ("SNOPA") sought to prohibit employers and schools from requiring or requesting that employees, students, and job applicants provide a username or password to access a personal account on any social networking website.<sup>57</sup> Similar to some of the state legislation, SNOPA would make it unlawful for an employer to discipline, deny, or discharge an employee or applicant who declined to provide such information.<sup>58</sup> SNOPA was reintroduced in February 2013.<sup>59</sup> Next, the Password Protection Act of 2012 sought to prohibit employers from requiring job applicants and employees to provide access to their personal "protected computer."<sup>60</sup> This bill was reintroduced in May 2013, with a few revisions, including an exemption if the employer is complying with the requirements of federal or state law, rules, regulations, or the rules of a self-regulatory organization.<sup>61</sup> Congress is currently considering the two acts.<sup>62</sup>

---

55. Assemb. B. 25, 2014 Leg., Reg. Sess. (Cal. 2014).

56. *Id.*

57. H.R. 5050, 112th Cong. (2012).

58. *Id.*

59. H.R. 537, 113th Cong. (2013).

60. H.R. 5684, 112th Cong. (2012).

61. H.R. 2077, 113th Cong. (2013); S. 1426, 113th Cong. (2013).

62. See H.R. 537, 113th Cong. (2013) (referred to House Committee on Education and the Workforce); H.R. 2077, 113th Cong. (2013) (referred to House Committee on the Judiciary).

### III. CLAIMS POTENTIALLY TRIGGERED WHEN SOCIAL MEDIA INFORMS A HIRING DECISION

Employers who review and use a candidate's online information in the hiring process expose themselves to a variety of discrimination claims. This section focuses on several equal employment laws—Title VII, the Age Discrimination in Employment Act, and state laws prohibiting lifestyle discrimination—and analyzes how these well-established means of protection apply to the practice of social media vetting.

#### A. *Seek and Ye Shall Find: Title VII Protections Against Religious Discrimination*

In a highly publicized lawsuit addressing employment discrimination based on the employer's internet search, C. Martin Gaskell ("Gaskell") claimed that the University of Kentucky ("UK") violated Title VII of the Civil Rights Act of 1964 when it decided not to hire him because of his religious beliefs.<sup>63</sup> Title VII prohibits employers from refusing to hire an applicant "because of" several protected classes, including "[an] individual's . . . religion."<sup>64</sup> Religion is defined in the Act as "all aspects of religious observance and practice, as well as belief, unless an employer demonstrates that he is unable to reasonably accommodate to an employee's or prospective employee's religious observance or practice without undue hardship on the conduct of the employer's business."<sup>65</sup> Under this section, a plaintiff may assert a claim of discrimination in the hiring process by showing either direct or indirect evidence.<sup>66</sup>

The case arose out of the 2007 search and selection of a founding director to oversee the new astronomical observatory at UK.<sup>67</sup> Of the twelve people who applied for the position, there was no dispute that Gaskell was a leading candidate based on his application.<sup>68</sup> Following

---

63. *Gaskell v. Univ. of Ky.*, No. 09-244-KSF, 2010 U.S. Dist. LEXIS 124572, at \*2 (E.D. Ky. Nov. 23, 2010).

64. 42 U.S.C. § 2000e-2(a) (2012).

65. 42 U.S.C. § 2000e(j).

66. *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*17.

67. *Id.* at \*1.

68. *Id.* at \*7.

review of the written applications, the UK Search Committee conducted phone interviews and ranked the leading candidates on an objective scale by assigning a number score to each of five job criteria.<sup>69</sup> Gaskell came in first.<sup>70</sup>

Despite Gaskell's "immense experience in virtually every aspect of the observatory director's duties," he was not hired.<sup>71</sup> Instead, UK hired a former student and employee of their Department of Physics & Astronomy, Timothy Knauer, who "demonstrated more of the qualities that UK wanted in its Observatory Director."<sup>72</sup> Gaskell, however, brought suit alleging employment discrimination based on the employer's Internet search.<sup>73</sup> During the search process, one of the search committee members "conducted an internet search for information about Gaskell" and found articles and lecture notes Gaskell posted on his personal website espousing "creationist" views.<sup>74</sup> Additionally, Gaskell pointed to an email written by the Search Committee Chair, Thomas Troland, just days prior to the committee's vote.<sup>75</sup> In the email, Troland complained that Gaskell would be denied the job "'because of his religious beliefs,' that 'no objective observer could possibly believe,' the decision was based on any reason other than religion," and, "that the whole process caus[ed] him to question UK's commitment to 'religious freedom.'"<sup>76</sup>

There, the district court held that when Gaskell's allegations were "considered together and taken as true, [they raised] a triable issue of fact as to whether his religious beliefs were a substantial motivating factor in UK's decision not to hire him."<sup>77</sup> The direct evidence of religious discrimination led the court to deny both Gaskell's and UK's motions for

---

69. *Id.* at \*8.

70. *Id.*

71. *Id.* at \*22.

72. *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*1-2.

73. *Id.* at \*10-11.

74. *Id.*

75. *Id.* at \*21.

76. *Id.* at \*14, \*21-22.

77. *Id.* at \*25.

summary judgment.<sup>78</sup>

Although the *Gaskell* case did not involve a direct demand for an applicant's social media account access, the case illustrates how an employment discrimination claim may arise under Title VII in the context of an employer discovering and unlawfully using an applicant's online information in its hiring decision.<sup>79</sup> Aside from prohibitions on religious discrimination, Title VII also states it is unlawful for an employer:

- (1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin; or
- (2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's race, color, religion, sex, or national origin.<sup>80</sup>

Social media screening creates a greater possibility of disparate treatment (treating an applicant differently because of a protected class status) than many other selection methods due to protected class status information prevalent on social media sites not otherwise gleaned from a resume.<sup>81</sup> Several studies exploiting minor variations in the content of resumes have established that employers use information that signals membership in certain groups to discriminate against applicants.<sup>82</sup> A

---

78. *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*26, \*30.

79. *Id.* at \*28–30.

80. 42 U.S.C. § 2000e-2(a)(1)-(2) (2012).

81. Donald H. Kluemper, *Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection*, in 12 ADVANCED SERIES IN MANAGEMENT: SOCIAL MEDIA IN HUMAN RESOURCES MANAGEMENT 1, 5 (Tanya Bondarouk & Miguel R. Olivas-Juján eds., 2013).

82. Devah Pager, *The Use of Field Experiments for Studies of Employment Discrimination: Contributions, Critiques, and Directions for the Future*, 609 ANNALS AM. ACAD. POL. & SOC. SCI. 104, 110-11 (2007), available at <http://ann.sagepub.com/content/609/1/104.full.pdf+html>.

traditional job application may not provide information about the race of the applicant, the applicant's sexual orientation, or his or her religious beliefs or political views. Yet social media could provide this information directly (e.g., a picture or a statement) or indirectly (e.g., membership in a group). Social media users self-report a wide range of personal details, including sexual orientation, relationship status, birth date, religious beliefs, and political affiliation.<sup>83</sup> The robust information available on social media makes it easy to see how other Title VII protected classes can be easily recognized in the online screening context.

### B. ADEA Prohibition of Age Discrimination

While Title VII includes a number of broad prohibitions on discrimination, the Act left untouched a considerable issue: discrimination based upon age. In response to this major problem, Congress enacted the Age Discrimination in Employment Act of 1967 ("ADEA") to "promote the employment of older persons" based on ability, "to prohibit arbitrary age discrimination," and to aid in studying the relationship between age and employment.<sup>84</sup> The 1967 Act protected only private sector employees between the ages of 40 and 65.<sup>85</sup> The 1974 amendment to the ADEA extended the protection of the Act to federal, state, and local government employees.<sup>86</sup>

In another employment discrimination lawsuit based on the employer's Internet search, Jason Nieman, a litigation and claims manager, claimed that Integrity Mutual Insurance Company ("Integrity") violated the ADEA when it decided not to hire him because of his age.<sup>87</sup> Nieman, who was forty-two at the time of his candidacy, alleged Integrity "followed the industry norm and used the Internet to research" him and discovered his online LinkedIn profile, which showed his college graduation date.<sup>88</sup> The

---

83. Kluemper, *supra* note 81, at 6.

84. 29 U.S.C. § 621(b) (2012).

85. 29 U.S.C. § 631 (2012).

86. Equal Emp't Opportunity Comm'n v. Elrod, 674 F.2d 601, 604 n.2 (7th Cir. 1982).

87. Nieman v. Grange Mut. Ins. Co., No. 11-3404, 2013 U.S. Dist. LEXIS 47685, at \*1 (C.D. Ill. Apr. 2, 2013).

88. *Id.* at \*16, \*19, \*38.



relevant section of the ADEA reads: “It shall be unlawful for an employer . . . to fail or refuse to hire or to discharge any individual or otherwise discriminate against any individual . . . because of such individual’s age[.]”<sup>89</sup> As previously mentioned, a plaintiff may assert a claim of discrimination in the hiring process through either direct or indirect evidence.<sup>90</sup>

The controversy began in February 2009 when Integrity conducted a search for a new Vice President of Claims (“VP of Claims”).<sup>91</sup> One hundred and thirty-three candidates applied for the position, including Nieman.<sup>92</sup> Cindy Heindel, who managed the search and conducted all phone screens, phone screened Nieman in February 2011 for less than one hour.<sup>93</sup> A month later, an Integrity recruiter emailed Heindel a list of five candidates by rank.<sup>94</sup> Nieman’s name was not on the list.<sup>95</sup> The search ended in June 2011 with the selection of Christian Martin, who was thirty-nine years old at the time.<sup>96</sup>

Nieman admitted he did not have any direct evidence of age discrimination.<sup>97</sup> However, under the indirect method, a plaintiff may establish a prima facie age discrimination in an employment case “by showing that he (1) was a member of a protected class, (2) sought a position for which he was qualified, (3) was not hired, and (4) a substantially younger person who was similarly situated was hired.”<sup>98</sup>

Integrity argued that Heindel neither conducted nor utilized an Internet search for any VP of Claims candidate, including Nieman.<sup>99</sup>

---

89. 29 U.S.C. § 623(a)(1) (2012).

90. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*29.

91. *Id.* at \*3–4.

92. *Id.* at \*4.

93. *Id.* at \*4, 7.

94. *Id.* at \*14.

95. *Id.*

96. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*6.

97. *Id.* at \*30.

98. *Id.* at \*34.

99. *Id.* at \*16.

Despite Nieman's dispute of nearly every assertion put forth by Integrity, the court concluded that Nieman's age discrimination claim failed for two reasons.<sup>100</sup> First, Nieman was unqualified.<sup>101</sup> Heindel testified that she had decided to disqualify Nieman during the phone screen because he was long-winded in his answers, interrupted her, and gave poor examples of corporate impact for employers.<sup>102</sup> Though the record established that Nieman had "whatever basic qualifications Integrity required to be interviewed for the position,"<sup>103</sup> Martin had "superior communication skills and excellent strategic skills."<sup>104</sup> The court reasoned that "it is entirely appropriate for an employer to subjectively analyze the varying traits of each applicant."<sup>105</sup> Second, Martin was not "substantially younger."<sup>106</sup> The three-year age gap between Martin and Nieman was insufficient to establish this element, which generally requires a ten-year age difference.<sup>107</sup> Based on the foregoing, the court granted Integrity's motion for summary judgment.<sup>108</sup>

In contrast to *Gaskell*, where the plaintiff successfully produced direct evidence to establish an employment discrimination claim based on the employer's Internet search,<sup>109</sup> the *Nieman* case demonstrates an instance of how a plaintiff's discrimination claim against an employer can ultimately fail.<sup>110</sup> Although *Gaskell* discussed religious discrimination<sup>111</sup> and *Nieman*

---

100. *Id.* at \*35–39.

101. *Id.* at \*37.

102. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*8.

103. *Id.* at \*35.

104. *Id.* at \*22.

105. *Id.* at \*35 (internal quotation marks omitted).

106. *Id.* at \*37.

107. *Id.* at \*38.

108. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*39.

109. *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*10.

110. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*69.

111. *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*3.

alleged age discrimination,<sup>112</sup> the two cases are comparable because of their underlying premise: the unlawful use of an applicant's information, obtained through an employer's Internet search, in the hiring decision.<sup>113</sup> The two district courts applied a typical nondiscrimination test—a plaintiff may assert a claim of discrimination in the hiring process by showing either direct or indirect evidence—to cases where discriminatory information is discovered online.<sup>114</sup> In *Nieman*, the plaintiff lacked any direct evidence of age discrimination,<sup>115</sup> and Integrity denied conducting an Internet search.<sup>116</sup> In contrast, the defendant in *Gaskell* conceded to discovering<sup>117</sup> and disagreeing with Gaskell's religious views on his personal web site.<sup>118</sup> Although Nieman could have alleged a valid claim by relying upon other evidence, he offered “nothing more than his own speculation” about the discrimination.<sup>119</sup> Indeed, nine of the twelve candidates who received interviews after the phone screen were older than Nieman.<sup>120</sup> Furthermore, the VP of Claims position was originally offered to and declined by Jim Blair in May 2009, who was fifty-seven at the time.<sup>121</sup>

A job candidate may never be certain of the reasons for which they were not hired.<sup>122</sup> As one employment website stated, these types of cases

---

112. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*1.

113. *Id.* at \*16; *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*23–25.

114. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*29; *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*17.

115. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*30.

116. *Id.* at \*30.

117. *Gaskell*, 2010 U.S. Dist. LEXIS 124572, at \*10–11.

118. *See id.* at \*21–22.

119. *Nieman*, 2013 U.S. Dist. LEXIS 47685, at \*39.

120. *Id.* at \*5.

121. *Id.* at \*6.

122. Lisa Guerin, *Lawsuits Based on the Hiring Process*, NOLO, <http://www.nolo.com/legal-encyclopedia/lawsuits-based-the-hiring-process.html> (last visited Mar. 29, 2015).

are “hard to know—and harder to prove.”<sup>123</sup> Nevertheless, *Gaskell* and *Nieman* demonstrate how pre-employment Internet screening exposes the employer to liability based on information discovered online, whether from a social media page or a personal blog. As in *Nieman*, often times an applicant is left with strong suspicions of unlawful discrimination but little hard evidence. However, an applicant could, at the very least, file a Title VII<sup>124</sup> or ADEA<sup>125</sup> claim for discrimination when an employer discovers protected information through a basic Internet search during the hiring process.

### C. State Prohibitions on Lifestyle Discrimination

In addition to these two major federal pieces of legislation, a number of states offer somewhat broader protection against employment discrimination by enacting laws banning so-called “lifestyle discrimination.”<sup>126</sup> As law professor Stephen Sugarman points out, some off-duty conduct can endanger the employer’s financial interests.<sup>127</sup> Sugarman explains that an employer may justify a decision not to hire an applicant because of his or her lifestyle “on the ground that the consequences of the off-duty behavior in some way spill over to the workplace, affecting the employer’s legitimate interests.”<sup>128</sup> The employer is motivated, therefore, to avoid hiring an applicant whose behavior might cause interpersonal strife among employees, decrease productivity, tarnish the company’s reputation, or incur extra financial burdens.<sup>129</sup> Lifestyle behaviors that can clash with an employer’s legitimate interests include the employee’s personal relationships (e.g., having an extramarital affair),<sup>130</sup>

---

123. *Id.*

124. *See* 42 U.S.C. § 2000e-2(a) (2012).

125. *See* 29 U.S.C. § 623(a) (2012).

126. *See* Stephen D. Sugarman, “Lifestyle” Discrimination in Employment, 24 BERKELEY J. EMP. & LAB. L. 377, 416 (2003).

127. *Id.* at 383.

128. *Id.* at 379.

129. *Id.* at 383.

130. *Id.* at 384–88.

civic or political activities (e.g., complaining to a government agency about a private employer's working conditions),<sup>131</sup> dangerous leisure activities (e.g., hang-gliding),<sup>132</sup> daily habits (e.g., drinking and smoking),<sup>133</sup> and illegal acts committed off-duty.<sup>134</sup>

Lifestyle discrimination statutes protect an employee's or applicant's use of lawful products or participation in lawful off-duty activities, conduct, or speech. State prohibitions on lifestyle discrimination add yet another layer of anti-employment discrimination legislation that is particularly relevant to employers gathering information through social media vetting, especially because social media sites are so full of records documenting a prospective employee's lifestyle.<sup>135</sup> For example, Facebook photos of an applicant speaking out at a public hearing or posing with a beer and smoking a cigarette are direct evidence of the applicant's lifestyle choices which, in some states, are illegal bases upon which to make a hiring decision.<sup>136</sup>

#### IV. THE IMPACT AND SIGNIFICANCE OF AN EVOLVING SOCIAL MEDIA LEGAL LANDSCAPE

##### A. *Pending Social Media Legislation*

Pending social media legislation attempts to fill in the gaps left by the majority of current state social media laws that only prevent employers from asking an applicant for his or her social media username and password. Even if an employer does not ask prospective employees for their social media login credentials, employers can gain access to these websites through a variety of other methods.

---

131. *See id.* at 388–89.

132. *See* Sugarman, *supra* note 126, at 389–90.

133. *See id.* at 391–92.

134. *See id.* at 393–95.

135. *See* Brian Lamoureux, *Social Media Privacy Law Impacts Employers*, PROVIDENCE BUSINESS NEWS (July 21, 2014), <http://www.pldw.com/Knowledge-and-Resource-Center/Social-media-privacy-law-impacts-employers.pdf>.

136. *See* Sugarman, *supra* note 126, at 416–20.

## 1. “Shoulder Surfing”

In some cases, employers may ask applicants to login to their social media profile in the presence of a supervisor, allowing the supervisor to review the contents of the applicant’s site at that time.<sup>137</sup> This practice, known as “‘shoulder surfing,’ might seem less intrusive than asking for a social media password,”<sup>138</sup> but it still conflicts with the intent of the recent laws designed to protect applicants’ online privacy.<sup>139</sup> Physically standing behind a prospective employee after he has logged-on to his social media account, and then forcing the employee to explore his social media network, still enables the employer to view protected information that state social media laws fight to protect.<sup>140</sup> In addition to the eleven bills that contain provisions prohibiting employers from requiring applicants to access their personal social media in the presence of the employer, shoulder surfing has already been made illegal in California, Illinois, Oregon, Rhode Island, and Washington.<sup>141</sup> California’s social media law specifies that employers cannot require employees to provide them with “any personal social media.”<sup>142</sup> Michigan’s social media 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 media account.<sup>143</sup> Prohibiting access to the content of the account, rather than just the username and password, makes shoulder surfing a nonissue.<sup>144</sup> Social

---

137. Martha C. White, *Facebook Weighs In and Blasts ‘Shoulder Surfing’ by Employers*, TIME (Mar. 23, 2012), <http://business.time.com/2012/03/23/facebook-weighs-in-and-blasts-shoulder-surfing-by-employers/>.

138. Robert T. Quackenboss, *Lesser-Known Social Media Legislation*, RISK MGMT. (Oct. 1, 2013, 10:50 AM), <http://www.rmmagazine.com/2013/10/01/lesser-known-social-media-legislation>.

139. *Id.*

140. *See id.*

141. *Id.*; Brian Lamoureux, *Social Media Privacy Law Impacts Employers*, PROVIDENCE BUSINESS NEWS (July 21, 2014), <http://www.pldw.com/Knowledge-and-Resource-Center/Social-media-privacy-law-impacts-employers.pdf>.

142. 2012-A.B. 1844 Cal. Adv. Legis. Serv. Ch. 618 (LexisNexis).

143. H.B. 5523, 96th Leg., 2012 Reg. Sess. (Mich. 2011).

144. *See* Kristin Cifolelli, *Warning: Friending Subordinates Can Lead to Trouble*,

media laws that do not focus on the protection of private information as a whole are under-inclusive in regards to loopholes that turn the issue from “what” information is gathered to “how.”

## 2. Mandatory “Friending”

In other cases, employers may side-step password protection laws by requiring the applicant to “friend” a staff member of the employer, thereby allowing that individual access to the information on the social media site.<sup>145</sup> If an employer or supervisor is included on an applicant’s contact list, they can view content that the applicant posts to the social media network.<sup>146</sup> Once an employer is a social media “friend,” they no longer need to shoulder surf or request a password, because they can log on with their own account and see what the applicant has posted.<sup>147</sup>

Ten states have pending legislation that would ban requiring applicants to connect with either an employer or a supervisor on social media networks.<sup>148</sup> Mandatory friending has already been outlawed in Rhode Island,<sup>149</sup> Arkansas, Colorado, Oregon, and Washington.<sup>150</sup> In Arkansas, the law prohibits even requesting or suggesting that an employee or applicant friend an employer or supervisor.<sup>151</sup> In Colorado, Oregon, and Washington, a friend request that an employee sends to an employer is permitted, as long as the employee or applicant is not coerced or otherwise

---

AMERICAN SOCIETY OF EMPLOYERS (July 16, 2014),  
<https://www.aseonline.org/ArticleDetailsPage/tabid/7442/ArticleID/944/Warning-Friending-Subordinates-Can-Lead-to-Trouble.aspx>.

145. *Id.*

146. *See NYC May Bar Social Media Demands By Employers*, ASSOCIATED PRESS (Sept. 26, 2013, 12:44 PM), [http://www.crainsnewyork.com/article/20130926/PROFESSIONAL\\_SERVICES/130929917/nyc-may-bar-social-media-demands-by-employers](http://www.crainsnewyork.com/article/20130926/PROFESSIONAL_SERVICES/130929917/nyc-may-bar-social-media-demands-by-employers).

147. Quackenboss, *supra* note 138.

148. *Id.*

149. Lamoureux, *supra* note 141.

150. Quackenboss, *supra* note 138.

151. H.B. 1901, 89th Gen. Assemb., Reg. Sess. (Ark. 2013).

required to accept the request.<sup>152</sup> This ban, however, creates a special challenge for professional networking sites where personal profiles are designed with the intention of networking for job opportunities.<sup>153</sup> The ban does not tailor to distinct social media platforms, such as Facebook and LinkedIn, in which the major differences between the two likely prompt distinct issues.<sup>154</sup> “Facebook (when compared to LinkedIn) has more users, generally has more information, is typically geared toward ‘friends’ (rather than professional ‘connections’), has a greater ability to restrict access,” and is the focus of recent legislation.<sup>155</sup> LinkedIn, on the other hand, is akin to an expanded resume and, “is used for the explicit purpose of connecting professionally, including that of recruitment and selection.”<sup>156</sup> A blanket ban on friending employees “creates special challenges with professional networking applications such as LinkedIn, where colleagues might naturally expect to connect with one another despite a hierarchical differential between supervisor and employee.”<sup>157</sup>

### 3. Social Media Privacy Settings

Finally, some legislatures have protected employee privacy by enacting legislation that prevents employers from requiring that applicants change the privacy settings on their social media network to make their profile publicly available.<sup>158</sup> Some social media sites offer privacy settings that permit users to control access to their personal social media pages.<sup>159</sup> Privacy settings differ from website to website.<sup>160</sup> On the more

---

152. Quackenboss, *supra* note 138.

153. *Id.*

154. Donald H. Kluemper, *Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection*, in 12 *ADVANCED SERIES IN MANAGEMENT: SOCIAL MEDIA IN HUMAN RESOURCES MANAGEMENT* 1, 8–9 (Miguel R. Olivas-Juján & Tanya Bondarouk eds., 2013).

155. *Id.* at 9.

156. *Id.*

157. Quackenboss, *supra* note 138.

158. *Id.*

159. *Social Networking Privacy: How to be Safe, Secure and Social*, PRIVACY RIGHTS CLEARINGHOUSE, <https://www.privacyrights.org/social-networking-privacy-how-be-safe-secure-and-social> (last modified Feb. 2015).



public end of the spectrum, privacy settings for Twitter and YouTube are publicly visible by default.<sup>161</sup> Upon creating a Twitter account, a new user's profile and tweets are open to public view, along with the list of "followers" and those "followed."<sup>162</sup> The default setting for YouTube is that anyone can see a new user's profile and videos, anyone can comment on the user's videos, and anyone can message the user.<sup>163</sup> To repeat: default settings can be modified.<sup>164</sup>

In an attempt to keep up with the popularity of micropublishing sites like Twitter, Facebook made "Public" the default setting for its 350 million users in December 2009.<sup>165</sup> The sweeping new privacy settings automatically published status updates, photos, videos, and friends lists to anyone on and off Facebook, unless modified otherwise.<sup>166</sup> Facebook founder and CEO Mark Zuckerberg explained the change as a reflection of the "social norm" at the time: "[p]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people."<sup>167</sup> Despite Facebook's intent to give users more control over their information, civil liberties campaigners such as the ACLU and the Electronic Frontier Foundation were outraged and called the

---

160. See generally *Social Media Security and Privacy Settings*, INDEP. BUS. OWNERS ASS'N INT'L, <http://www.iboai.com/index.php/en/social-media/social-media-security-and-privacy-settings> (last visited Mar. 29, 2015) (explaining the different privacy settings and options of popular social media websites).

161. *Id.*

162. *Id.*

163. *Id.*

164. See *id.* ("You can change [default] settings if you choose . . .").

165. Bobbie Johnson, *Facebook Privacy Change Angers Campaigners*, THE GUARDIAN (Dec. 10, 2009, 1:42 PM), <http://www.theguardian.com/technology/2009/dec/10/facebook-privacy>; Ryan Singel, *Public Posting Now the Default on Facebook*, WIRED (Dec. 9, 2009, 2:33 PM), <http://www.wired.com/2009/12/facebook-privacy-update/>.

166. Johnson, *supra* note 165; Larry Magid, *Facebook Details New Privacy Settings*, CNET (Dec. 9, 2009, 7:25 AM), <http://www.cnet.com/news/facebook-details-new-privacy-settings/> (discussing that the "maximum exposure available to users under 18 will be friends of friends or school networks").

167. Marshall Kirkpatrick, *Facebook's Zuckerberg Says The Age of Privacy is Over*, READWRITE (Jan. 9, 2010), [http://readwrite.com/2010/01/09/facebook\\_zuckerberg\\_says\\_the\\_age\\_of\\_privacy\\_is\\_ov](http://readwrite.com/2010/01/09/facebook_zuckerberg_says_the_age_of_privacy_is_ov).

developments “flawed,” “worrisome,” and “plain ugly.”<sup>168</sup> In May 2014, Facebook bowed to privacy concerns and reversed its default settings for new users so that, going forward, the default setting is “Friends” instead of “Public.”<sup>169</sup> Facebook’s new intent to protect users from over-sharing is an about-face on its privacy policy of just five years earlier.<sup>170</sup>

Lastly, on the very private end of the spectrum, LinkedIn requires users to accept requests in order to connect and will often ask for the other person’s email address to verify that users know whom they are requesting.<sup>171</sup> Unlike Twitter, YouTube, and Facebook, LinkedIn privatizes information by default and highly recommends that users do not connect with people they do not know.<sup>172</sup> According to one study, fifteen percent of Facebook users (nearly one hundred and fifty million users), seven percent of LinkedIn users (nearly fifteen million users), and five percent of Twitter users (more than twenty seven million) modified privacy settings, specifically with work in mind.<sup>173</sup> While users of social media are resorting to privacy settings to screen their social activity from others, many of the existing social media laws do not prevent an employer from demanding that a prospective employee not place the employer behind an online privacy wall.<sup>174</sup> Pending legislation about the issue includes six state bills that contain provisions prohibiting employers from requiring, requesting, or even suggesting that an applicant change the privacy settings on his or her social media network.<sup>175</sup> Arkansas, Colorado, Rhode Island,

---

168. Johnson, *supra* note 165.

169. Doug Gross, *Facebook Privacy Now Defaults to Friends Only*, CNN (May 22, 2014, 3:39 PM), <http://www.cnn.com/2014/05/22/tech/social-media/facebook-privacy/>.

170. Todd Wasserman, *Facebook Switches Default Setting to Private to Prevent Oversharing*, MASHABLE (May 22, 2014), <http://mashable.com/2014/05/22/facebook-private-default-setting/>.

171. *Social Media Security and Privacy Settings*, *supra* note 160.

172. *Id.*

173. Phillip L. Gordon, Amber M. Spataro & William J. Simmons, *Social Media Password Protection and Privacy—The Patchwork of State Laws and How It Affects Employers*, LITTLER 1, 2 (May 2013), <http://www.littler.com/files/press/pdf/WPI-Social-Media-Password-Protection-Privacy-May-2013.pdf>.

174. Quackenboss, *supra* note 138.

175. *Id.*

and Washington have enacted this provision into law.<sup>176</sup>

In short, by over-the-shoulder surfing while a prospective employee explores his or her social media profile, connecting to a prospective employee through social media, or requiring an applicant to change his or her privacy settings, an employer does not break the social media law in many states.

### *B. Legislation Versus Self-Regulation*

Due to the rapid evolution of technology, distinct social media legislation has been substantially outpaced by organizational practice, yielding laws that are simultaneously over-inclusive, under-inclusive, and all-around insufficient.<sup>177</sup> Instead, these issues would be best cured by a “firm-defined regulation” model of self-regulation, given the dynamic nature of the problem, the fact that many of these relationships will be cross-state relationships (at least initially), and because the optimal rule may vary according to the type of industry and business.<sup>178</sup>

The term “self-regulation” covers a range of regulatory systems, each with varying degrees of government involvement and industry responsibilities.<sup>179</sup> Self-regulation should be used when the public interest requires regulation itself.<sup>180</sup> As a starting point, a problem must exist that can be solved or ameliorated by regulation; without that threshold question being answered in the affirmative, self-regulation should not be considered.<sup>181</sup> In the context of social media pre-employment screening, the public interest requires regulation, as evidenced by developing social media laws focusing on privacy protection and equal employment.<sup>182</sup>

---

176. *Id.*; see also Lamoureux, *supra* note 141.

177. See Lisa Quast, *Social Media, Passwords, and the Hiring Process: Privacy and Other Legal Rights*, FORBES (May 28, 2012, 8:56 AM), <http://www.forbes.com/sites/lisaquast/2012/05/28/social-media-passwords-and-the-hiring-process-privacy-and-other-legal-rights/2/>.

178. Margot Priest, *The Privatization of Regulation: Five Models of Self-Regulation*, 29 OTTAWA L. REV. 233, 256–58 (1997-1998).

179. *Id.* at 237.

180. *Id.* at 298.

181. *Id.*

182. *Id.*

However, as this Note explored, legislative efforts banning employers' access to passwords as well as pending legislation designed to protect social media information are insufficient to cure the various problems arising from employer use of social media screening. Password protection laws enacted to date overlap, but also contradict each other in a variety of ways—shoulder surfing, mandatory friending, and changing privacy settings illustrate only three of the numerous nuances to the issue.<sup>183</sup> Employers at home in multiple states must be made aware of, and updated on, laws at both the local and federal levels, along with potential penalties.<sup>184</sup> Employers must continue to balance their business interests with applicants' privacy rights as they manage their workforce.<sup>185</sup>

Firm-defined regulation would be advantageous to employers and prospective employees alike because of the model's flexibility, lower costs, commitment to the rules, and more comprehensive rules.<sup>186</sup> In addition, more individualistic and tailored rules to a particular industry could foster innovative solutions to novel issues.<sup>187</sup> The bottom-line is this: assuming employers choose to screen prospective employees' social media, they should take steps internally to rectify the situation.<sup>188</sup> That is to say, instead of continuing to approach employer use of social media vetting in the hiring process with "one size fits all" legislation, the issue should be cured with self-regulation where a company may tailor rules and practices specific to its industry and needs.<sup>189</sup>

---

183. Gordon, Spataro & Simmons, *supra* note 173, at 10.

184. *See supra* Parts II.C, III.A–B.

185. *See supra* Part III.C.

186. *See* Priest, *supra* note 178, at 257.

187. *Id.*

188. *See id.* at 257–58 (“There are more internal inspectors in firms (usually for quality control) than any government inspectorate could hope to muster, and internal inspectors may have powers (such as entrapment) that government inspectors lack.”).

189. *See id.* at 258 (“Incentives are also available to an internal inspectorate that are lacking for government.”).

### C. Proposed Best Practice Guidelines

#### 1. Social Media Screening Policy

Employers should use social media only “as one of many tools and sources of information available in the hiring process.”<sup>190</sup> Employers should pursue intelligent policies that effectively leverage relevant information from social media to supplement their selection of qualified candidates.<sup>191</sup> An employer’s senior management, legal department, and human resources (“HR”) should work together to build social media into an existing screening policy.<sup>192</sup> Through collaboration, senior management can determine what the company is looking for and the goals of social media screening; lawyers can specify which online information can be gathered and lawfully relied upon in the hiring process; and HR can set strict Internet search procedures and implement proper screening software.<sup>193</sup>

Generally, the information obtained and requested through the pre-employment process should be limited to those essential in determining whether a person is qualified for the job.<sup>194</sup> Indeed, screening criteria that fails to be job-related and consistent with business necessity serves little purpose in an employment selection.<sup>195</sup> Tailoring a search in proportion to the sensitivity of the job position would curtail an employer’s exposure to unlawful information. Information regarding race, sex, national origin,

---

190. Quast, *supra* note 177.

191. *See id.*

192. *See* James Hardwood, *Employees, Human Resources and Social Media Best Practices—Top Questions to Consider*, TOTAL HR, <http://www.totalhrmanagement.com/employees-human-resources-and-social-media-best-practices-top-questions-to-consider> (last visited Mar. 29, 2015).

193. *See id.*

194. *See Prohibited Employment Policies/Practices*, U.S. EQUAL EMP’T OPPORTUNITY COMM’N, [http://www.eeoc.gov/laws/practices/index.cfm#pre-employment\\_inquiries](http://www.eeoc.gov/laws/practices/index.cfm#pre-employment_inquiries) (last visited Mar. 29, 2015); Stacy A. Hickox & Mark V. Roehling, *Negative Credentials: Fair and Effective Consideration of Criminal Records*, 50 AM. BUS. L.J. 201, 213 (2013) (“Best practice in [human resource management] provides that before a selection test or criterion can be used to assess applicants and make hiring decisions, there must be reasonable evidence that it is a valid predictor for the job(s) in question.”).

195. Kluemper, *supra* note 154, at 7.

age, and religion are irrelevant in employment determinations.<sup>196</sup> Additionally, inquiries about organizations, clubs, and societies in which an applicant may be a member that may indicate the applicant's race, sex, national origin, disability status, age, religion, color or ancestry, should also generally be avoided.<sup>197</sup> An effective policy would specifically describe proper Internet screening procedures, proscribe obtaining fraudulent access to private information, and prohibit consideration of protected classes or other unlawful factors that may be revealed.

## 2. Hire a Third-Party Agency

Hiring a third-party agency, as a non-decision maker, to conduct the social media screen is beneficial for at least three reasons. First, manually assessing candidates' social media is time-consuming and cumbersome when comparing across candidates.<sup>198</sup> Additionally, "it is a challenge to derive useful information, such as passion around a particular technology or relevant professional connections."<sup>199</sup> Hiring an outside agency that will filter through integrated social media data can relieve this burden and save time.<sup>200</sup> Reppify, for example, is a leading third-party service-provider that "helps employers screen potential candidates, including via online presence through the candidates' social media networks."<sup>201</sup>

Second, insulating the "information gatherer" from the "information user" adds a buffer that helps avoid unintentional legal violations.<sup>202</sup> When the information gatherer is also the decision maker, that person is doomed to discover unlawful information that may influence the employment decision simply by virtue of that approach's structure.<sup>203</sup> Automatic

---

196. *Prohibited Employment Policies/Practices*, supra note 194.

197. *Id.*

198. Quast, supra note 177.

199. *Id.*

200. *Id.*

201. *Id.*

202. See Dr. Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 561–62 (2013).

203. *Id.*

exposure to protected class information creates a basis upon which a plaintiff could allege employment discrimination.<sup>204</sup> Thus, a third-party information gatherer is in a better position to redact all protected characteristics and other unlawful information from the report.<sup>205</sup> Reppify CEO Chirag Nangia explained:

Today, employers perform web searches on candidates, learn more about them from social media, and examine their work samples. These processes introduce noise and are potentially risky . . . To ensure no ethical or legal boundaries are crossed, our proprietary technology removes the noise, such as Protected Class data, ensuring both the privacy of the job seeker is protected while helping the employer get a better perspective on the best candidates for the position.<sup>206</sup>

After an employer specifies which criteria to screen, Reppify screens, scores, and ranks the candidates.<sup>207</sup> This two-layered structure leads to more consistent, criteria-based results.<sup>208</sup>

Third, specialized Internet screening agencies possess expertise in this evolving area of law. Whereas the Fair Credit Reporting Act (“FCRA”) does not cover information that an employer gathers independently, including information from informal Internet searches, the FCRA applies to employers using third-party screening companies.<sup>209</sup> Therefore, these

---

204. *Id.* at 562.

205. For example, the United States Equal Employment Opportunity Commission advises employers not to ask for a photograph of an applicant. In addition to redacting unlawful information, screening reports would prevent viewing photos that normally accompany social media profiles. *Prohibited Employment Policies/Practices*, *supra* note 194.

206. Quast, *supra* note 177.

207. Reppify, *How Reppify Works*, YOUTUBE (Sept. 17, 2012), <http://www.youtube.com/watch?v=5TrXm-YXPq4>.

208. *Id.*

209. See *Social Networking Privacy: How to be Safe, Secure, and Social*, *supra* note 159 (“The Fair Credit Reporting Act (FCRA) is a law that not only regulates credit reports but also sets national standards for employment screening and background checks. In effect, it sets limits on what information employers can get from background checks and how they can use that

outsourced screening companies become experts in their practice.<sup>210</sup> Reppify boasts that its screening procedure complies with the FCRA, undergoes data verification, and helps minimize liability for negligent hiring and discrimination claims.<sup>211</sup> Of course, as this Note proposes, a sophisticated employer with the resources and legal expertise to develop a social media screening policy might fully comply with all applicable state and federal equal employment laws. Nevertheless, a third-party approach appears most prudent for employers because of the complex application and rapidly developing area of social media law.<sup>212</sup>

### 3. Consistency is Key

Consistent treatment of all job applicants, across all protected groups, prevents disparate treatment of any individual.<sup>213</sup> Employer screening policies should be consistent throughout the process in order to safeguard against bias.<sup>214</sup> Internet background searches of each and every applicant, rather than on a case-by-case basis, can be evidence of equal screening.<sup>215</sup> Employers should document each search to show the screen was properly performed and narrowly tailored. This documentation should include the sites visited, the findings from each site, and the findings ultimately used in making the hiring decision. Thorough documentation showing proper screening procedures and legitimate, nondiscriminatory findings may provide a shield to a negligent hire action as well as employment discrimination lawsuits.<sup>216</sup> Furthermore, employers should proactively

---

information . . . However, the FCRA only applies to employers using third-party screening companies. Information that an employer gathers independently, including from informal Internet searches, is not covered by the FCRA.”).

210. See Ghoshray, *supra* note 202, at 561–62.

211. Reppify, *supra* note 207.

212. Quast, *supra* note 177.

213. Hickox & Roehling, *supra* note 194, at 211.

214. *Id.* at 259.

215. See Bill Glenn, *Employing Social Media Best Practices*, GLOBAL BUS. NEWS, <http://www.globalbusinessnews.net/story.asp?sid=1590> (last visited Mar. 29, 2015).

216. *Id.*



train HR personnel and hiring managers on the applicable laws.<sup>217</sup> Companies that try to “adhere to the same standards set forth by the FCRA will ultimately be in a better position to make their case for using social media during the hiring process.”<sup>218</sup> Consistent, on-going training and counsel from experienced employment lawyers will ensure that companies comply with existing and emerging statutory, regulatory, and case law.<sup>219</sup>

## V. CONCLUSION

Social media pre-employment screening during the hiring process is an evolving legal landscape that increases the risk of employers unlawfully discriminating against applicants using information found online.<sup>220</sup> Employers using social media in the hiring process should know that existing equal employment and privacy law concepts apply to the social media space, in addition to new applicable state social media legislation. Any information gathered from the Internet should be used consistently with non-discriminatory hiring policies and practices. Since inherent risks of inaccuracy, misinterpretation, and lack of verifiable data on social media can compromise any screen,<sup>221</sup> setting strict Internet search procedures and consistent application, or otherwise hiring a third-party vendor, are optimal self-regulatory approaches for employers to both maintain business interests and prevent legal liabilities.<sup>222</sup>

---

217. Quast, *supra* note 177.

218. Glenn, *supra* note 215.

219. Quast, *supra* note 177.

220. See generally Bill Glenn, *Employing Social Media Best Practices*, GLOBAL BUS. NEWS, <http://www.globalbusinessnews.net/story.asp?sid=1590> (last visited Mar. 29, 2015) (noting that the increased use of social media has led to a subsequent increase in screening potential job candidates through those platforms, leading to both advantages and disadvantages for employers).

221. Donald H. Kluemper, *Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection*, in 12 ADVANCED SERIES IN MANAGEMENT: SOCIAL MEDIA IN HUMAN RESOURCES MANAGEMENT 1, 8 (Tanya Bondarouk & Miguel R. Olivas-Juján eds., 2013) (discussing the concepts of validity, reliability, and generalizability as they relate to social media screening in various occupations).

222. See Dr. Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 561–62 (2013).