

1-1-2014

## Striking Gold, Not Dynamite When Using Social Media in Employment Screening

Mark Bannister

Michael Jilka

Derek Ulrich

Follow this and additional works at: <http://scholarlycommons.law.hofstra.edu/hlelj>

 Part of the [Labor and Employment Law Commons](#)

---

### Recommended Citation

Bannister, Mark; Jilka, Michael; and Ulrich, Derek (2014) "Striking Gold, Not Dynamite When Using Social Media in Employment Screening," *Hofstra Labor & Employment Law Journal*: Vol. 32: Iss. 1, Article 1.  
Available at: <http://scholarlycommons.law.hofstra.edu/hlelj/vol32/iss1/1>

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Labor & Employment Law Journal by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact [lawcls@hofstra.edu](mailto:lawcls@hofstra.edu).

## ARTICLES

### STRIKING GOLD, NOT DYNAMITE WHEN USING SOCIAL MEDIA IN EMPLOYMENT SCREENING

*Mark Bannister,\* Michael Jilka,\*\* Derek Ulrich\*\*\**

#### I. OVERVIEW

Recruiting and selecting the best, most qualified, and productive employees possible is a crucial process for businesses and other organizations seeking to run smoothly and to stay competitive.<sup>1</sup> A potential employee's skills, experiences, and work ethic should appropriately align with the employer-organization's vital needs.<sup>2</sup> Finding relevant information about job applicants and making decisions based on such information is a routine step in employment screening.<sup>3</sup>

Nearly one-half of the United States population is a member of a

---

\* Mark Bannister is the Dean of the College of Business and Entrepreneurship at Fort Hays State University. The college offers significant business, information technology, and media programs at the undergraduate and graduate levels on-campus, through domestic distance learning and international partnerships. He is a Senior Policy Fellow of the Docking Institute of Public Affairs and a principal in Bannister Capital Advisers. He teaches courses on such subjects as "Law of Cyberspace" and has published in a number of law and business journals. Dean Bannister is a graduate of the University of Kansas School of Law.

\*\* Michael Jilka is a partner in Nichols Jilka LLP, based in Lawrence, Kansas. He is a graduate of the University of Kansas School of Law. Michael clerked for the Kansas Court of Appeals and U.S. District Judge Monti Belot, served as an Assistant Attorney General, and practiced litigation in the Kansas City area before starting his own law firm. Jilka has published numerous articles in the Kansas Bar Journal on topics ranging from civil rights litigation, search and seizure, the First Amendment, and attorney's fees.

\*\*\* Derek Ulrich is a first year law student at the University of Kansas School of Law. He has worked as a student research assistant working with Dean Bannister.

1. See MARY F. COOK & ASSOCIATES ET AL., *THE AMA HANDBOOK FOR EMPLOYEE RECRUITMENT AND RETENTION 2* (Mary F. Cook ed., Am. Mgmt. Ass'n 1992).

2. See Axelrod, E.L. et al., *War for talent, Part Two*, *THE MCKINSEY QUARTERLY*, April 2001 at 9-11 available at <http://www.veruspartners.net/private/app/webroot/files/wata01.pdf>.

3. See *id.*

social media site.<sup>4</sup> Such sites are rich with personal information. A growing percentage of employers are screening social media in the employment process and many are finding useful information.<sup>5</sup> However, use of social media can run afoul of federal and state laws on discrimination and other specialized statutes addressing requests for IDs and passwords, life style activities, consumer credit, and records retention.<sup>6</sup> This article examines the use of social media searches and the attendant advantages, potential legal pitfalls, and potential protective strategies employers may use when searching social media during the employee selection process.<sup>7</sup>

## II. THE POWER OF THE INTERNET – EMPLOYERS TURN TO GOOGLE AND SOCIAL MEDIA

Internet search engines such as Google are extremely powerful. Search engines scan and catalogue enormous amounts of data<sup>8</sup> including the burgeoning resource of personal information known as “social media,” a search engine’s power can be harnessed with a few keystrokes, listing pages of links on any subject—including the name of a job applicant.<sup>9</sup> Kaplan and Haenlein define social media as “a group

---

4. See Jay Baer, *11 Shocking New Social Media Statistics in America*, CONVINCE & CONVERT, <http://www.convinceandconvert.com/social-media-research/11-shocking-new-social-media-statistics-in-america/> (last visited Sept. 20, 2014).

5. See Jennifer Grasz, *Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds*, CAREERBUILDER (Aug. 19, 2009), [http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009%siteid=cbpr&sc\\_cmp1=cb\\_pr519\\_](http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8%2f19%2f2009&ed=12%2f31%2f2009%siteid=cbpr&sc_cmp1=cb_pr519_).

6. Recent news stories about employer abuse of Facebook and other social media focus on employer activities after the hiring decision. E.g., Howard M. Bloom & Philip B. Rosen, *Firings for Facebook Comments Unlawful, NLRB Rules*, ACC (Sept. 8, 2014), <https://www.lexology.com/library/detail.aspx?g=429e1e02-25cc-4da7-84d3-2f32781a2362>. While compelling, these stories are outside the scope of this article.

7. See *infra* Part V.B, Part VII-XI.

8. See Gary Marcus, *The Web Gets Smarter*, THE NEW YORKER (May 23, 2012), <http://www.newyorker.com/online/blogs/culture/2012/05/google-knowledge-graph.html> (noting Google has one of the largest collections of computers in the world, wired up in parallel, housing some of the largest databases in the world. Your search queries can be answered so quickly because they are outsourced to immense data farms, which then draw upon enormous amounts of precompiled data, accumulated every second by millions of virtual Google ‘spiders’ that crawl the Web).

9. See Cecilia Kang, *Google Announces Privacy Changes Across Products and Users Can’t Opt Out*, THE WASHINGTON POST (Jan. 24, 2012), [http://www.washingtonpost.com/business/economy/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQAArgJHOQ\\_story.html](http://www.washingtonpost.com/business/economy/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQAArgJHOQ_story.html). Google changed its privacy policies in March 2012 allowing it to link the accounts of users across its many platforms. *Id.* The change allows Google to track its users Internet activities and collect and index data about them. *Id.*

of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of User Generated Content.”<sup>10</sup> By early 2014, North American social media sites had hundreds of millions of users, and the number world-wide reached more than 1.15 billion<sup>11</sup> utilizing any number of social media sites.<sup>12</sup> These included specialized social media sites, such as Flickr (photo sharing)<sup>13</sup> and Linked-In (professional networking),<sup>14</sup> as well as more general use social media sites, such as Friendster,<sup>15</sup> Facebook,<sup>16</sup> Twitter<sup>17</sup> and Google+.<sup>18</sup> Each of these sites potentially contains information that can help an employer learn more about a potential employee than a cover letter, résumé, or perhaps even a face-to-face interview.<sup>19</sup>

With more than 1.32 billion users—more than half of which log in daily—Facebook currently reigns as the Internet’s largest social media site.<sup>20</sup> Approximately nineteen percent of Facebook’s users are located

10. Andreas M. Kaplan & Michael Haenlein, *Users of the World, Unite! The Challenges and Opportunities of Social Media*, 53 BUS. HORIZONS 59, 61 (2010). Kaplan and Haenlein identify six different types of social media: collaborative projects (e.g., Wikipedia), blogs and microblogs (e.g., Twitter), content communities (e.g., YouTube), social networking sites (e.g., Facebook), virtual game worlds (e.g., World of Warcraft), and virtual social worlds (e.g., Second Life). *Id.* at 62.

11. Facebook alone had 1.23 billion monthly active users as of December 31, 2013; it had 757 million daily users. Ami Sedghi, *Facebook: 10 years of Social Networking, in Numbers*, DATABLOG (Feb. 4, 2014 9:38 AM), <http://www.theguardian.com/news/datablog/2014/feb/04/facebook-in-numbers-statistics>.

Approximately 81.7% of daily users are outside the U.S. and Canada. *Our Mission*, FACEBOOK NEWSROOM, <http://newsroom.fb.com/company-info/> (last visited Feb. 9, 2014).

12. See, e.g., *Number of Facebook Users Worldwide from 3<sup>rd</sup> Quarter 2008 to 2<sup>nd</sup> Quarter 2014 (in millions)*, STATISTA, <http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (last visited Sept. 16, 2014).

13. *About Flickr*, FLICKR <https://www.flickr.com/about> (last visited Feb. 9, 2014). One of Flickr’s main goals is “to help people make their photos available to the people who matter to them.” *Id.*

14. LINKEDIN, <http://www.linkedin.com/> (last visited Feb. 9, 2014).

15. FRIENDSTER, <http://www.friendster.com/> (last visited Feb. 9, 2014).

16. FACEBOOK, <http://www.facebook.com/> (last visited Feb. 9, 2014).

17. TWITTER, <https://twitter.com/> (last visited Feb. 9, 2014).

18. GOOGLE+, <http://www.google.com/+> (last visited Feb. 9, 2014).

19. See *Privacy Policy*, GOOGLE (Mar. 31, 2014), <http://www.google.com/policies/privacy/>.

It is worthwhile to note that many users are members of more than a single site. Personally identifiable data stored across several sites can be found and aggregated when properly employing a search engine’s search logic and tools. Google, which owns several social media sites, recently changed its privacy policies that permit it to link data across site by a user’s unique identity for the ostensible purpose of providing a better online experience for its users and its social media sites’ members. *Id.*

20. *Our Mission*, *supra* note 11; see also Cooper Smith, *The Planet’s 24 Largest Social Media Sites and Where Their Next Wave of Growth Will Come From*, BUSINESS INSIDER (Nov. 29, 2013 3:20 PM), <http://www.businessinsider.com/a-global-social-media-census-2013-10>.

in North American as of June 2014.<sup>21</sup> Nearly forty percent of the United States population use Facebook daily.<sup>22</sup> Facebook permits members to create personal profiles which may contain any assortment of personal data the member wishes to share. As of February 2014, Facebook offered users thirty-six different categories for posting information.<sup>23</sup> A driving feature of Facebook is its “timeline”—a place in the member’s profile to which updates of the member’s “status” can be posted.<sup>24</sup> Sharing these updates with others creates the social aspect of the site. These updates are not limited to text-based messages; similar to its social media peers, Facebook is media rich—full of photos and sometimes videos posted by members.<sup>25</sup> “On average more than 350 million photos per day were uploaded on to Facebook in the fourth quarter of 2012.”<sup>26</sup> Other areas in the member’s profile often contain substantial information about the member. Links to news, sports, entertainment, and other items of interest can be quickly added by members to their timeline, and commentary about the link can be added.<sup>27</sup>

It is the sharing of and commenting upon these posted bits of information by users that makes the social experience. When a member makes a social connection through Facebook, the member is said to “friend” the contact, which results in Facebook including the new contact in a public list of the individual’s “friends.”<sup>28</sup> “Friends” in the list can include both people and organizations, potentially revealing information about a person’s associates and interests. Facebook will share information with a member’s friends when the member chooses to “like” another member’s statements, photos, videos, books, websites, organizations, and other categories.<sup>29</sup> Members are alerted to any

---

21. *Our Mission*, *supra* note 11.

22. Kurt Wagner, *More Than 40% of Americans Use Facebook Every day*, MASHABLE (Aug. 13, 2013), <http://mashable.com/2013/08/13/40-percent-americans-use-facebook-every-day/>.

23. See *What is My Profile?*, FACEBOOK (July 2014), <https://www.facebook.com/help/www/133986550032744>.

24. See *Introducing Timeline*, FACEBOOK, <https://www.facebook.com/about/timeline> (last visited Sept. 27, 2014).

25. See *What is My Profile?*, *supra* note 23.

26. Facebook, Inc., Annual Report (Form 10-K) 5 (Feb. 1, 2013) available at <http://files.shareholder.com/downloads/AMDA-NJ5DZ/2301311196x0xS1326801-13-3/1326801/1326801-13-3.pdf>.

27. See *What is My Profile?*, *supra* note 23.

28. See *Adding Friends & Friend Requests*, FACEBOOK (July 2014), <https://www.facebook.com/help/360212094049906/>.

29. See *Like*, FACEBOOK (July 2014), <https://www.facebook.com/help/452446998120360/>.

“likes” their postings generate.<sup>30</sup> Facebook can share with the member’s “friends” titles of music the member is currently listening to on Spotify, movies that are being watched on Netflix, or recently read on-line news articles.<sup>31</sup> As a result, Facebook potentially includes significant amounts of information about a possible employee, painting an extremely detailed picture of the applicant for the employer.

To access Facebook and the data it contains about a member, an employer must be a member.<sup>32</sup> Once a member, Facebook provides its own search tool and allows members to search by name, city, and current or former employer. Search engines such as Google and Bing can sweep the Web and point to the social media accounts of users.<sup>33</sup>

A substantial number of employers are searching social media.<sup>34</sup> A 2013 study by CareerBuilder.Com found that nearly thirty-nine percent of employers use social media websites to research job applicants.<sup>35</sup> This is up from thirty-seven percent from 2012.<sup>36</sup> Forty-three percent of those surveyed have these found information they report led them not to hire a candidate “such as provocative or inappropriate photos and discriminatory comments related to race, gender or religion or the like—while nineteen percent said they have found information that influenced their decision to hire a candidate—such as evidence of great communications skills and a professional-looking profile.”<sup>37</sup> The *New York Times* reports that some organizations actively search LinkedIn and Facebook networks of employees friends to find potential applicants.<sup>38</sup>

From the job applicant standpoint, savvy entrepreneurs and career services offices at colleges, universities, professional schools, and internet job hunting sites offer advice to help people manage and clean their online profiles.<sup>39</sup> If potential employees expand their “brand”

---

30. *Id.*

31. See *Follow*, FACEBOOK (Apr. 2014), <https://www.facebook.com/help/382751108453953/>.

32. See *Search for Friends on Facebook*, FACEBOOK, <https://www.facebook.com/srch.php> (last visited Sept. 15, 2014).

33. See *Privacy Settings and Tools*, FACEBOOK, <https://www.facebook.com/settings/?tab=privacy> (last visited Sept. 15, 2014).

34. See Mary Lorenz, *Two in Five Employers Use Social Media to Screen Candidates*, CAREERBUILDER (July 1, 2013), <https://thehiringsite.careerbuilder.com/2013/07/01/two-in-five-employers-use-social-media-to-screen-candidates/>.

35. *Id.*

36. *Id.*

37. *Id.*

38. Julie Weed, *Finding New Employees, via Social Networks*, NY TIMES, (May 31, 2009), <http://www.nytimes.com/2009/05/31/jobs/31recruit.html>.

39. See Allan Hoffman, *How to Clean Up Your Online Reputation*, MONSTER, <http://career-advice.monster.com/job-search/getting-started/clean-up-your-online-reputation/article.aspx> (last

through social media and employers in turn screen candidates through social media, employers must comply with applicable federal and state laws prohibiting employment discrimination and with a variety of other relevant state and federal laws.<sup>40</sup>

### III. FEDERAL EMPLOYMENT DISCRIMINATION ACTS

#### A. Overview

A suite of United States federal acts address employment discrimination. Title VII of the Civil Rights Act of 1964 ("Title VII") is the most broad-sweeping of these acts. It deems it to be "an unlawful employment practice for an employer—(1) to fail or refuse to hire or 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, sex, or national origin."<sup>41</sup> The Americans with Disabilities Act ("ADA") prohibits discrimination against individuals based on disability.<sup>42</sup> The ADA prohibits employers from discriminating against individuals on "the basis of disability in regard to job application procedures and hiring."<sup>43</sup> The Age Discrimination in Employment Act ("ADEA") prohibits employment discrimination against persons 40 years of age or older.<sup>44</sup> Together these acts form the nucleus of anti-discriminatory protections extended to job applicants and employees.

These federal acts define the terms "employer" and "employee."<sup>45</sup> Title VII and the ADA apply to employers "engaged in an industry affecting commerce who have fifteen or more employees for each working day in each of twenty or more calendar weeks in the current or preceding calendar year, and any agent of such a person," with limited exceptions.<sup>46</sup> "Employee" means an individual employed by an

---

visited Feb. 9, 2014); Clair Prentice, *Online Profile Spring Cleaning*, BBC NEWS (Sept. 24, 2010), <http://www.bbc.co.uk/news/technology-11381037>. Reppler is an example of a company that advertises its services to help manage clients' social media images. *About TrustedID Reppler*, TRUSTEDID, <http://www.reppler.com/about/> (last visited Feb. 9, 2014).

40. Ed Walters, *Social Media Discrimination*, FASTCASE (Apr. 15, 2011), <http://www.fastcase.com/social-media-discrimination/>.

41. Civil Rights Act of 1964, 42 U.S.C. § 2000e(2)(a) (2012).

42. ADA Amendments Act of 2008, Pub. L. No. 110-325, 122 Stat. 3553, § 2(a)(1) (2008).

43. Americans with Disabilities Act, 42 U.S.C. § 12112(a) (2006).

44. Age Discrimination in Employment Act of 1967, 29 U.S.C.S. § 621 631 (LexisNexis 2002).

45. 42 U.S.C. § 2000e(b), (f) (2006); 42 U.S.C. § 12111(4), (5)(a) (2006).

46. 42 U.S.C. § 2000e(a) (2006); *See also* 42 U.S.C. § 12111(5)(A) (2006).

employer,” except for certain political-employees.<sup>47</sup> The ADEA utilizes similar definitions, yet it applies only to employers with twenty or more employees.<sup>48</sup> States typically have employment discrimination acts paralleling these federal frameworks.

### B. *Pre-Employment Screening under Federal Employment Acts*

Charged with enforcement of these federal acts, the Equal Employment Opportunity Commission (“EEOC”) provides compliance guidance to employers.<sup>49</sup> The EEOC’s guidance on pre-employment inquiries seeks to avoid inadvertent violation by employers of Title VII protections by indicating prohibited questions regarding a number of potentially discriminatory topics.<sup>50</sup> For example, an employer may not ask: about arrest records (inquiries into convictions are acceptable if job-related); any inquiry about religious observance; about child care—unless asked of all of applicants; about birthplace, national origin, ancestry, or lineage of applicant, applicant’s parents, or applicant’s spouse, applicant’s religious affiliation, church parish or religious holidays observed—unless religion is a bona fide occupational qualification; marital status, number and age of children, or spouse’s job; height and weight—unless related to job requirements; military type or condition of discharge; organizations a candidate belongs to—unless they are professional organizations related to the job; requiring photographs except after hiring; any inquiry into pregnancy, medical history of pregnancy or family plans; applicant’s race or color of skin; or sex unless it is a bona fide occupational qualification.<sup>51</sup>

An EEOC publication guides an employer away from discrimination and towards ADA compliance by warning that employers are prohibited from asking disability related questions until after making a conditional job offer.<sup>52</sup> As for ADEA compliance, the EEOC warns,

[T]he ADEA does not specifically prohibit an employer from asking an applicant’s age or date of birth. However, because such inquiries may deter older workers from applying for employment or may

47. 42 U.S.C. § 2000e(f) (2006).

48. Age Discrimination in Employment Act of 1967, 29 U.S.C.A. § 630 (b).

49. Overview, U.S. EEOC, <http://eeoc.gov/eeoc/index.cfm> (last visited Sept. 24, 2014).

50. *Prohibited Employment Policies/Practices*, U.S. EEOC, <http://www.eeoc.gov/laws/practices> (last visited Sept. 24, 2014).

51. *Id.*

52. See EEOC, *Enforcement Guidance: Pre-Employment Disability Related Questions and Medical Examinations*, U.S. EEOC (Oct. 10, 1995), <http://www.eeoc.gov/policy/docs/preemp.html>.

otherwise indicate possible intent to discriminate based on age, requests for age information will be closely scrutinized to make sure that the inquiry was made for a lawful purpose, rather than for a purpose prohibited by the ADEA. If the information is needed for a lawful purpose, it can be obtained after the employee is hired.<sup>53</sup>

Though prohibited by these federal acts from directly gaining access to this information through an interview, an employer intent on discovering answers to proscribed questions may use access to the applicant's social media accounts to satisfy many—if not most—of its inquiries.

#### IV. FACEBOOK INQUIRIES

##### A. Information Control

Social media, such as Facebook, provides the opportunity for employers to gather information significantly beyond résumés and interviews. Facebook members share personal and professional information with inner circles of friends, other members, and often the general public.<sup>54</sup> Information availability varies considerably, with each member ostensibly controlling the availability, and thus the level of privacy, for shared items.<sup>55</sup> Facebook's privacy statement assures "Facebook is designed to make it easy for you to share your information with anyone you want. You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings."<sup>56</sup>

Prior to becoming a member and posting and sharing information, a Facebook member must assent to an end-user agreement and Facebook's terms of service.<sup>57</sup> The terms of service discloses to users the extent that information potentially may be shared. These state in part:

When you use an application, the application may ask for your permission to access your content and information as well as content

---

53. *Fact Sheet*, U.S. EEOC (Dec. 28, 2009), <http://www.eeoc.gov/eeoc/publications/upload/age.pdf>.

54. See Facebook, Inc., *supra* note 26 at 5; see *Our Mission*, *supra* note 11.

55. *Privacy Settings and Tools*, *supra* note 33.

56. *Facebook's Privacy Policy*, FACEBOOK (Oct. 29, 2009), [https://www.facebook.com/note.php?note\\_id=%20322194465300](https://www.facebook.com/note.php?note_id=%20322194465300).

57. See *Statement of Rights and Responsibilities*, FACEBOOK (Nov. 15, 2013), <https://www.facebook.com/legal/terms>.

and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information.<sup>58</sup>

When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).<sup>59</sup>

The typical Facebook member has neither read the end-user agreement nor is aware of privacy settings.<sup>60</sup> Many do not restrict access to posted information.<sup>61</sup> One study of Facebook members from a large northeast university found that only 11.3% of students restricted access to their Facebook profile.<sup>62</sup> These privacy settings are a key tool controlling access to member information.

Four general privacy settings—"Public," "Friends," "Only Me," and "Custom"<sup>63</sup>—enable members to reveal or conceal information to friends and the general public. With the most conservative, minimal setting, a public non-friend member searching for a name may find only a profile with a name and the regional city with which the user is identified.<sup>64</sup> A profile photo may also be returned by the search since most Facebook members share at least that additional piece of information for identification purposes.<sup>65</sup> Those members not employing stringent privacy or sharing settings allow other information to be returned in a search, such as current employer, and schools

---

58. *Id.* An "application" is a third party software or utility used by Facebook members to be social. These "apps" can be used to share calendars, identify biological and legal relatives, and play games. *See Id.* In the latter use, the apps encourage "friending" in order to increase game scores or gain or implement strategies. *See Games Overview*, FACEBOOK, <https://developers.facebook.com/docs/games/overview> (last visited Sept. 15, 2014).

59. *Statement of Rights and Responsibilities*, *supra* note 57.

60. A 2005 study that assessed consumer computer security knowledge found that only 6.4% of the respondents who download shareware read end-user agreements, with another 4% reading "most" of such agreements. *See* Xiaoni Zhang, *What Do Consumers Really Know*, 48 COMM'NS OF THE ACM, no. 8, Aug. 2005 at 44, 47.

61. *See* Ethan Kolek & Daniel Saunders, *Online Disclosure: An Empirical Examination of Undergraduate Facebook Profiles*, 45 NASPA J. 1, 13 (2008).

62. *Id.*

63. Joe Donovan, *How to Set Facebook Privacy Settings*, DIGITALTREND (Mar. 26, 2014), <http://www.digitaltrends.com/social-media/how-to-set-facebook-privacy-settings/>.

64. *See id.*

65. A profile photo can be anything a member desires. These can include the typical photo of the member's face (which can reveal a great deal of discriminatory information), a photo of the member and a significant other, a family photo, a cartoon, or a political advertisement.

attended (secondary, universities, etc.).<sup>66</sup> However, many members willingly share their complete profile with the public which includes such personal information as birth date,<sup>67</sup> “in relationship with,”<sup>68</sup> “Likes,”<sup>69</sup> and multiple folders of photos.<sup>70</sup> A member can choose to restrict most information categories to friends, which is a blunt means of controlling information.<sup>71</sup> Other more sophisticated members can deftly permit and deny access to information using a combination of controls and tools.<sup>72</sup>

Unless a member employs tools to create more restrictive circles, limiting profile and information access to a member’s “Friends” allows those same Facebook friends access to most, if not all information a member posts.<sup>73</sup> This provides, at best, a false sense of information security because “Friends” in most cases may be able to repost (and thus share) a member’s information (such as photos) with anyone the “Friend” chooses.<sup>74</sup> To be sure, there are social benefits to posting. Many members post their birthdates and enjoy the cascade of well wishes on their birthdays.<sup>75</sup> Many members list their relationship status and identify the person with whom the relationship exists.<sup>76</sup> Many members also post photos as a way to share the activities in their lives.<sup>77</sup> Members can also “Like” companies, musicians, movies, books, products, politicians, political movements or organizations, churches, and statements or postings made by other members.<sup>78</sup> All of this information, some of which may be considered by the member as

---

66. Donovan, *supra* note 63.

67. This can provide discriminatory information related to age.

68. This can provide discriminatory information related to marital status, religion, and sexual orientation.

69. This information can provide a wealth of information which can lead to inferences about membership in protected classes.

70. Only one’s imagination limits what information may be gleaned from a review of photos.

71. See Donovan, *supra* note 63.

72. See *id.*

73. See *id.*

74. Facebook’s Privacy Policy – Full Version, *supra* note 56.

75. See Meagan Choi, *Why Some People Don’t Want Birthday Greetings on Facebook*, CNN (Aug. 12, 2011, 7:10 AM), <http://www.cnn.com/2011/TECH/social.media/08/12/facebook.birthday.popularity/index.html>.

76. See *Global Number of Changes of the Relationship Status on Facebook in 2010*, STATISTA (Jan. 2011), <http://www.statista.com/statistics/270927/changes-of-the-relationship-status-on-facebook/>.

77. *What is Facebook?*, GCF LEARNFREE.ORG, <http://www.gcflernfree.org/facebook101/2.2> (last visited Sept. 25, 2014).

78. See *Likes, Comments and Resharing*, GCF LEARNFREE.ORG, <http://www.gcflernfree.org/facebook101/6.3> (last visited Sept. 25, 2014).

“private,” can ultimately escape a close circle of friends by the inherent sharing nature of social media.

Information revealed on a member’s Facebook site may come from sources other than the member. Herein lies a hidden danger. Friends can post comments on the member-friend’s timeline.<sup>79</sup> These friends can also “tag” the people shown in a photo or other information that they have posted.<sup>80</sup> These tagged items may show up on the member’s site. In varying versions of Facebook, it has been relatively easy to almost impossible to remove postings and tagged photos.<sup>81</sup> Because of this feature, an interested employer can now access a wide variety of information about potential applicants that such applicants may not intend to share. When the inherent information distribution features of social media combine with the unwillingness of users to self-educate about these features that limit information, potential legal employment discrimination problems appear.

In addition to the openness and the *per se* easy availability of information on social media, even restricted information may be made available if a job seeker receives a “friend” request from someone with whom he or she has just interviewed. The applicant will likely feel compelled to accept the friend request in order to continue to build relationships with the potential new boss or new colleague.<sup>82</sup> Likewise, if researching a potential employer via its Facebook site, a potential employee may decide to “Friend” the employer, thus voluntarily exposing information limited to “Friends.”<sup>83</sup> With the “friend” relationship established, the potential employer may gain greater access to the applicant’s information.<sup>84</sup>

### B. Potentially Relevant Information

Many employers actively use the information gained from public profiles in the hiring process.<sup>85</sup> A 2013 CareerBuilder.Com survey of

---

79. *Id.*

80. See *Timeline and Tagging Settings*, GCF LEARNFREE.ORG, <http://www.gcfllearnfree.org/facebook101/5.3> (last visited Sept. 25, 2014).

81. See *The Audience Selector*, GCF LEARNFREE.ORG, <http://www.gcfllearnfree.org/facebook101/5.2> (last visited Sept. 25, 2014).

82. See Kate Rogers, *Help! My Boss Friend Requested Me on Facebook*, FOX BUSINESS (Mar. 29, 2012), <http://smallbusiness.foxbusiness.com/legal-hr/2012/03/29/help-my-boss-friend-requested-me-on-facebook/>.

83. Donovan, *supra* note 63.

84. Facebook’s Privacy Policy – Full Version, *supra* note 56.

85. See *More Employers Finding Reasons Not to Hire Candidates on Social Media*,

hiring managers found that forty-three percent of those who used social media to research candidates have found valid information that has caused them not to hire a candidate.<sup>86</sup> Reasons for candidate rejections included the following:

- Candidate posted provocative/inappropriate photos/info – 50%
- There was info about candidate drinking or using drugs – 48%
- Candidate bad mouthed previous employer – 33%
- Candidate had poor communication skills – 30%
- Candidate made discriminatory comments related to race, gender, religion, etc. – 28%
- Candidate lied about qualifications – 24%<sup>87</sup>

Conversely, the same study found that 19% of hiring managers have found content on social networking sites that convinced them to hire the candidate.<sup>88</sup> The top examples include the following:

- Candidate conveyed a professional image – 57%
- Got a good feel for candidate's personality – 50%
- Candidate was well-rounded, showed a wide range of interests – 50%
- Candidate's background information supported professional

---

*CareerBuilder Survey*, CAREERBUILDER (June 27, 2013), <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2013&id=pr766&ed=12%2F31%2F2013>. This survey was conducted online within the U.S. by Harris Interactive<sup>®</sup> on behalf of CareerBuilder among 2,184 hiring managers and human resource professionals (employed full-time, not self-employed, non-government) between February 11 and March 6, 2013 (percentages for some questions are based on a subset, based on their responses to certain questions). *Id.* With a pure probability sample of 2,184, one could say with a ninety-five percent probability that the overall results have a sampling error of +/- 2.1 percentage points. Sampling error for data from sub-samples is higher and varies.

86. *Id.*

87. *Id.*

88. *Id.*

qualifications – 49%

- Candidate was creative – 46%
- Great communication skills – 43%
- Other people posted great references about the candidate – 38%<sup>89</sup>

Information gathered on a member's Facebook site may be valuable and relevant to an employer for other reasons. A résumé can be vetted against an applicant's profile information for inconsistencies in academic and employment histories. Applicants with inappropriate racial, sexual, or otherwise discriminatory statements posted to their profile may be wisely eliminated from the candidate pool, as well as those exhibiting unwise or illegal activities in photos. All of these postings, whether text, photographic, links, or likes, paint a picture of the applicant. The CareerBuilder.com report summary concludes that "the research suggests that hiring managers are using social media to get a glimpse at the candidate's behavior and personality outside of the interview, and are most interested in professional presentation and how the candidate would fit with the company culture."<sup>90</sup>

A professional social media networking service such as LinkedIn is designed in part to help members "establish [their] professional profile" and "leverage powerful tools to find and reach the people [they] need."<sup>91</sup> LinkedIn also allows the building of "Groups" and of posting jobs within these networks – a very inexpensive means of reaching potential employees with certain skill sets and professional interests.<sup>92</sup> This type of service is valuable to both employers and potential employees as they seek to find each other.

### *C. Potentially Harmful Information*

There are practical drawbacks to employers gathering candidate information through social media. The practice may lead to drawing

---

89. *Id.*

90. *Id.*

91. *The Value of LinkedIn- LinkedIn Overview Video*, LINKEDIN (Sept. 26, 2013), [http://help.linkedin.com/app/answers/detail/a\\_id/45/~the-value-of-linkedin](http://help.linkedin.com/app/answers/detail/a_id/45/~the-value-of-linkedin).

92. *E.g.*, Fort Hays State University maintains a FHSU MBA Group connecting current MBA students and alumni. *Fort Hays State University MBA*, LINKEDIN, <http://www.linkedin.com/groups?gid=2562862> (last visited Sept. 16, 2014).

incorrect conclusions based on posted information or taking as truthful statements intentionally posted in an inaccurate manner or in jest. Inaccurate information may pale in comparison to the potential for mistaken identity. A search on Facebook for the name of a colleague of one of the authors found eleven members, including two from the individual's hometown. Celebrities and common people alike have suffered from the creation of faux sites.<sup>93</sup> Bill Gates is one celebrity that has suffered from fake sites.<sup>94</sup> In a 2012 regulatory filing, Facebook estimated that eighty-three million or 8.7% of its active users are duplicate or false accounts.<sup>95</sup> The problem's significance generated a Facebook fan page demanding verification of celebrity and corporate Facebook sites<sup>96</sup> and prompted Facebook to provide a mechanism for reporting fake accounts.<sup>97</sup> A contrasting type of now defunct business - MyFaceWall.com suggested that it allows you to "easily create fake profile pages just for fun."<sup>98</sup>

Two recent cases illustrate the potential harm of falsifying Facebook profiles. In what is considered one of the more notorious cases, a California man created 130 fake Facebook profiles to harass his former girlfriend.<sup>99</sup> He made additional postings to Craigslist with the girl's name and explicit photos.<sup>100</sup> In New Jersey, a woman impersonated her ex-boyfriend and posted inflammatory comments on a fake Facebook site.<sup>101</sup> Comments on the fake profile suggested the boyfriend (a police detective) frequented prostitutes, had a sexually

---

93. See *Friend Me: Celebrities' Fake Facebook Pages*, GEEKOLOGIE (Apr. 5, 2009), <http://geekologie.com/2009/04/friend-me-celebrities-fake-fac.php>.

94. *Id.*

95. See Heather Kelly, *83 Million Facebook Accounts are Fakes and Dupes*, CNN TECH, <http://www.cnn.com/2012/08/02/tech/social-media/facebook-fake-accounts> (last updated Aug. 2, 2012, 8:32 PM).

96. See *Facebook to Launch Verified Pages and Profiles for Brands and Celebrities*, TECHVOIZE (May 30, 2013), <http://www.techvoize.com/facebook-to-launch-verified-pages-and-profiles-for-brands-and-celebrities/>.

97. See *How do I Report a Fake Account?*, FACEBOOK HELP CENTER, <https://www.facebook.com/help/167722253287296> (last visited Feb. 9, 2014).

98. *Make Your Facebook Friend Fool with Fake Wall*, FACEBOOK (July 12, 2011), <http://www.facebook.com/onlinetipsguru/posts/163339190402392>.

99. See Katie Wiggin, *Calif. Man Creates 130 Fake Facebook Profiles to Harass Ex-girlfriend, Pleads No Contest*, CBS NEWS (Oct. 21, 2011, 4:25 PM), [http://www.cbsnews.com/8301-504083\\_162-20123755-504083/calif-man-creates-130-fake-facebook-profiles-to-harass-ex-girlfriend-pleads-no-contest/](http://www.cbsnews.com/8301-504083_162-20123755-504083/calif-man-creates-130-fake-facebook-profiles-to-harass-ex-girlfriend-pleads-no-contest/).

100. See *id.*

101. See David Porter, *Judge: Case of Fake Facebook Profile Can Proceed*, BOSTON.COM (Nov. 2, 2011), [http://www.boston.com/news/nation/articles/2011/11/02/judge\\_case\\_of\\_fake\\_facebook\\_profile\\_can\\_proceed/](http://www.boston.com/news/nation/articles/2011/11/02/judge_case_of_fake_facebook_profile_can_proceed/).

transmitted disease, and engaged in illegal drug use.<sup>102</sup>

Accidental mistakes can also occur. Tags of photos linked to the wrong person may be bothersome; tagged photos exhibiting intoxication or nudity linked to the wrong Facebook account can taint an innocent party. A comment posted on a wall in jest by a friend may be misinterpreted or damaging. The potential employer acting on what appears to be illegal activity or demonstrations of poor judgment, may be acting on fake or inaccurate material, ultimately leading the employer to pass over or disqualify a potentially valuable employee.

#### D. *Missing Information*

What if an applicant does not have a Facebook or any other social media account? A potential employer may have difficulty interpreting this void. It may be evidence of a very innocent background, a very busy person who does not participate in social media, or it may mean the applicant closed the accounts upon entering the job market, effectively hiding embarrassing or damaging information. One commentator, Tim Armstrong, suggests the absence may reflect “probity, circumspection, good judgment, and discretion. And to the extent that’s correct, it seems all to the good. On the other hand, perhaps what it shows is: technological unsophistication, ignorance, estrangement from the community of one’s peers, or an unhealthy self-absorption with one’s own public persona. . .”<sup>103</sup>

Armstrong continues:

The odds that twentysomethings who don’t post about their social exploits actually have fewer of them seem, to me at least, to be approximately zero. Hiring the person who doesn’t (currently) keep a blog or have a Facebook profile doesn’t say anything about whether the candidate’s actual background is squeaky-clean or not.<sup>104</sup>

### V. EMPLOYER DEMANDING USER NAMES AND PASSWORDS

#### A. *The Strategy and Controversy*

To eliminate the risk of accessing the wrong user’s data or that a

---

102. *See id.*

103. Tim Armstrong, *Social Darknets*, INFORMATION, LAW, & THE LAW OF INFORMATION (Jun. 12, 2006), <http://blogs.law.harvard.edu/infolaw/2006/06/12/social-darknets>.

104. *Id.*

potential employee is hiding information previously posted on social media accounts, some aggressive employers have started requesting social media site usernames and passwords from job applicants.<sup>105</sup> Employers received blistering publicity and were threatened with or subjected to legal action when they made such demands.<sup>106</sup> In 2009, the City of Bozeman, Montana, received considerable attention in both traditional and web-based media after a local television station reported the city government required job applicants to provide their usernames and passwords for “any and all, current personal or business websites, web pages or memberships on any internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc.”<sup>107</sup> The city was inundated with feedback and the City Manager quickly announced “[e]ffective at [noon] today . . . the City of Bozeman permanently ceased the practice of requesting candidates selected for City positions under a provisional job offer to provide user names or passwords for the candidate’s internet sites.”<sup>108</sup>

In 2011, the American Civil Liberties Union of Maryland (“ACLU”) jumped into the fray when the Maryland Department of Corrections (MDOC) required job applicant Robert Collins to provide his Facebook username and password.<sup>109</sup> MDOC defended its request, stating its need “to review wall postings, email communications, photographs, and friend lists, in order to ensure that those employed as corrections officers are not engaged in illegal activity or affiliated with

---

105. See Manuel Valdes & Shannon McFarland, *Employers Ask Job Seekers for Facebook Passwords*, YAHOO! NEWS (Mar. 20, 2012, 3:33 PM), <http://news.yahoo.com/employers-ask-job-seekers-facebook-passwords-170500338.html>.

106. See Denine K. Carr, *Do Employers Have the Right to Demand Social Media Passwords from Job Applicants and Employees?* 42 N.Y. ST. B. ASS’N TORTS, INS. & COMPENSATION L. SEC. J., 7- 8 (2013) (discussing the application of cases where juries found employers’ access to existing employees’ social media sites was unauthorized and violated a federal statute); see also *Employers, Schools, and Social Networking Privacy*, AM. CIV. LIBERTIES UNION (Apr. 24, 2012), <https://www.aclu.org/free-speech/employers-schools-and-social-networking-privacy> (highlighting recent popular examples of employers requesting passwords to private social networking accounts of job applicants, employees, and students).

107. Frederic Lardinois, *Want to Work for the City of Bozeman, MT? Hand Over Your Social Network Logins and Passwords*, READWRITE (June 18, 2009), [http://www.readwriteweb.com/archives/want\\_to\\_work\\_for\\_the\\_city\\_of\\_bozeman\\_mt\\_hand\\_over\\_passwords\\_login\\_info.php](http://www.readwriteweb.com/archives/want_to_work_for_the_city_of_bozeman_mt_hand_over_passwords_login_info.php).

108. *Id.*

109. See Letter from Deborah A. Jeon, Legal Dir., ACLU, to Gary D. Maynard, Sec’y, Md. Dep’t of Pub. Safety & Corr. Servs. (Jan. 25, 2011) (on file with ACLU), available at [http://www.aclu-md.org/uploaded\\_files/0000/004/letter\\_collins\\_final.pdf](http://www.aclu-md.org/uploaded_files/0000/004/letter_collins_final.pdf).

any gangs.”<sup>110</sup> The ACLU argued otherwise.

For social media users who maintain private accounts, the DOC demand for login information is equivalent to demands that they produce all of their private correspondence and photographs for review, or permit the government to listen in on their personal telephone calls, as a condition of employment. Such demands would be unconscionable, and there is no basis for treating electronic communications differently. While employers may permissibly incorporate some limited review of public internet postings into their background investigation procedures, review of password-protected materials overrides the privacy protections users have erected and thus violates their reasonable expectations of privacy in these communications.<sup>111</sup>

The ACLU further argued that the MDOC policy was illegal under the federal Stored Communications Act (“SCA”) and its Maryland state analog.<sup>112</sup> Among its prohibitions, the SCA forbids “intentionally access[ing] without authorization a facility through which an electronic communication service is provided”<sup>113</sup> The ACLU pointed to an unpublished opinion from the United States District Court of New Jersey, *Pietrylo v. Hillstone Restaurant Group*.<sup>114</sup> The *Pietrylo* decision awarded the employee-plaintiffs compensatory and punitive damages for SCA violations where the employer coerced an employee to surrender user credentials to a private, online forum.<sup>115</sup> After learning of a private Myspace chat room established by its employees where workplace grievances were aired, the employer (through one of its supervisors) successfully insisted an employee give up her identification and password.<sup>116</sup> Subsequently, the employer accessed and monitored the chat room.<sup>117</sup> Eventually, the employer fired the chat room’s creators for damaging employee morale and violating the restaurant’s “core values.”<sup>118</sup> The court opined if access to the chat room “was authorized ‘by a user of that service with respect to a communication of or intended

---

110. *Id.*

111. *Id.*

112. *Id.*; see 18 U.S.C. §§ 2701-2712 (2012); see also MD. CODE ANN., CTS. & JUD. PROC. §§ 10-4A-01 to -08 (West 2011).

113. 18 U.S.C. § 2701(a)(1).

114. See Letter from Deborah A. Jeon to Gary D. Maynard, *supra* note 109; see also *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754 (FSH), 2009 U.S. Dist. LEXIS 88702 (D. N.J.; Sept. 25, 2009).

115. See *Pietrylo*, 2009 U.S. Dist. LEXIS 88702, at \*2-3.

116. See *id.* at \*7-9.

117. See *id.* at \*10-11.

118. See *id.* at \*17-19.

for that user', there is no statutory violation."<sup>119</sup> However, the Court concluded a jury could reasonably infer from an employee's testimony that the "purported 'authorization' was coerced or provided under pressure," and thus, not authorized.<sup>120</sup>

After pressure from the ACLU and negative media regarding Collin's complaint, the MDOC announced on April 6, 2011, that it was revising its policy and would no longer require job applicants to provide social media identification and passwords—even though ninety-four percent of those hired in the past year felt compelled to provide this information.<sup>121</sup> While not all juries or courts may reach the same conclusion as the jury in *Pietrylo*, an employer runs a legal risk—potentially with punitive damages as well as a public relations risk—if it requires job applicants to provide social media identification and passwords. In response to these and other cases, several states have enacted or are considering laws banning this practice, with Maryland being the first to enact such legislation.<sup>122</sup> At the federal level, U.S. Senators Charles Schumer (N.Y.) and Richard Blumenthal (Conn.) requested the Department of Justice to investigate whether "this practice [of requesting user credentials from job applicants] violates the Stored Communications Act or the Computer Fraud and Abuse Act."<sup>123</sup>

## B. Statutory Restrictions on Employers Requests for Passwords

### 1. State Statutes Addressing IDs and Passwords

Legislation placing statutory limitations on employers' ability to demand the passwords of potential employees began to pass in 2012.<sup>124</sup> State legislative movement has been more rapid than that of Congress, but action is occurring on both levels. The thrust of most of these acts is that they protect some aspect of electronic and social media rights of

---

119. *Id.* at \*7.

120. *Id.* at \*9.

121. See *ACLU Responds To Maryland Division Of Corrections' Revision Of Invasive Social Media Policy*, ACLU (Apr. 6, 2011), <http://www.aclu.org/technology-and-liberty/aclu-responds-maryland-division-corrections-revision-invasive-social-media-po>.

122. See Sarah Breitenbach, *Md. Becomes First to Ok Password Protection Bill*, YAHOO! NEWS (Apr. 20, 2012, 10:10 AM), <http://news.yahoo.com/md-becomes-first-ok-password-protection-bill-113022373.html>.

123. Manuel Valdes, *Can Employers Ask For Applicants' Passwords?* THE WASHINGTON POST, Mar. 26, 2012, at A12.

124. See Md. Code Ann., Lab. & Empl. § 3-712(b)(1) (West 2013).

potential and current employees.<sup>125</sup> In 2012, four states enacted seminal laws restricting employers from seeking passwords to social media from job applicants.<sup>126</sup>

On May 2, 2012, Maryland enacted legislation prohibiting an employer from “request[ing] or requir[ing] that an employee or applicant disclose any username, password, or other means for accessing a personal account.”<sup>127</sup> The statute prohibits employers from taking disciplinary action against an employee or failing to hire an applicant for refusing to comply with such a request.<sup>128</sup>

Illinois followed Maryland with the passing of its Right to Privacy in the Workplace Act on August 1, 2012.<sup>129</sup> The Illinois statute differs from its predecessor in the language used. Whereas the Maryland statute prevents an employer from requiring access to “a personal account” in the employment screening process, the Illinois statute specifically addresses the privacy of social networking websites.<sup>130</sup> The Illinois statute makes it unlawful for an employer to request or require any “prospective employee to provide any password or other related account information in order to gain access to the employee’s or prospective employee’s account or profile on a social networking website.”<sup>131</sup> The Illinois statute defines social networking website as:

an Internet-based service that allows individuals to: (A) construct a public or semi-public profile within a bounded system, created by the service; (B) create a list of other users with whom they share a connection within the system; and (C) view and navigate their list of connections and those made by others within the system. “Social networking website” shall not include electronic mail.<sup>132</sup>

Importantly, the Illinois statute also states that “[n]othing in this subsection shall prohibit an employer from obtaining about a prospective employee or an employee information that is in the public domain.”<sup>133</sup> With this provision, the Illinois statute is the first statute to specifically

---

125. *See id.*

126. *See Employer Access to Social Media Usernames and Passwords*, 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>.

127. Lab. & Empl. § 3-712(b)(1).

128. *See id.* § 3-712(c)(1)-(c)(2) (2012).

129. 820 ILL. COMP. STAT. ANN. 55/10 (West 2014).

130. *See id.* § 55/10(b)(1).

131. *Id.*

132. *Id.* § 55/10(b)(4)(A)-(C).

133. *Id.* § 55/10(b)(3).

clarify that an employer can obtain information about a prospective employee that the employee or others have shared in the public domain.<sup>134</sup>

A little more than a month later, California became the third state to pass a law protecting social media privacy.<sup>135</sup> Like the Illinois statute, the California statute prevents an employer from requiring an applicant for employment to “disclose a username or password for the purpose of accessing personal social media.”<sup>136</sup> Additionally, it differs in that it expressly prohibits an employer from requiring or requesting “an employee or applicant for employment to . . . access personal social media in the presence of the employer.”<sup>137</sup> While the wording of the two previous statutes could be interpreted to include this activity, the California statute is the first to plainly prohibit this activity.<sup>138</sup>

In December 2012, Michigan passed its Internet Privacy Protection Act (“IPPA”).<sup>139</sup> The wording of this act is relatively broad and similar to Maryland’s. It does not permit an employer to “request an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the employee’s or applicant’s personal internet account.”<sup>140</sup> It prohibits an employer from failing to hire, or otherwise penalize “an applicant for employment for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the employee’s or applicant’s personal internet account.”<sup>141</sup>

Many other states have new or pending legislation that prohibit employers from requesting Internet and social media account information and passwords from job applicants. Ten states enacted legislation in 2013: Arkansas, Colorado, Illinois, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and Washington.<sup>142</sup> Overall

---

134. See *id.* § 55/10(b)(4)(A)-(C). Authority to obtain information does not necessarily shield an employer from liability if such information is used in a manner that contravenes laws on discrimination.

135. Ken Yeung, *California Becomes Third State to Protect Social Media Privacy*, TNW (Sept. 27, 2012, 8:34 PM), [thenextweb.com/insider/2012/09/27/California-social-media-privacy-law/](http://thenextweb.com/insider/2012/09/27/California-social-media-privacy-law/).

136. CAL. LAB. CODE § 980(b)(1) (West 2013).

137. *Id.* § 980(b)(2).

138. See *id.* § 980(b)(1)-(2).

139. H. R. 5523, 96th Leg., Reg. Sess. (Mich. 2012).

140. *Id.* § 3(a).

141. *Id.* § 3(b).

142. *Employer Access to Social Media Usernames and Passwords*, NAT’L CONF. OF ST. LEGISLATURES, <http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx> (last visited February 9, 2014).

thirty-six states had legislative activity on this topic in 2013.<sup>143</sup> Additional state enactments are probable.<sup>144</sup> Employers need to be aware of the statutory framework in the states in which they hire.

## 2. Federal Legislation on IDs and Passwords

Federal legislation would establish uniformity across the states and potentially preempt a patchwork of state laws. Two potential federal acts were introduced in the U.S. House of Representatives and one in the U.S. Senate in 2013.<sup>145</sup> These are very similar in structure to the state enactments and would prohibit an employer from requesting a user name and password to a social networking website or account.<sup>146</sup> None of the bills have moved beyond the initial committee they were assigned and they have a relatively small number of co-sponsors.<sup>147</sup> No bill appears to be close to passage as of the time that this article is being written in early 2014.

## VI. DISCRIMINATORY ACTIONS AFFECTING LEGALLY PROTECTED CLASSES

### A. Direct Discrimination

By searching Facebook or other social media sites, a potential employer may become exposed to not only information that may be useful and legitimate in employment decision making, they may also become aware of protected class information.<sup>148</sup> If an employer uses this

---

143. *Id.*

144. *See id.* As of February 9, 2014, legislation addressing employer access to social media usernames and passwords was pending in at least 28 states. *Id.*

145. *See* Social Networking Online Privacy Protection Act, H.R. 537, 113th Cong. (2013), available at <http://beta.congress.gov/bill/113th-congress/housebill/537?q=%7B%22search%22%3A%5B%22social+networking+online+protection+act%22%5D%7D>; *see also* Password Protection Act of 2013, H.R. 2077, 113th Cong. (2013), available at <http://beta.congress.gov/bill/113th-congress/house-bill/2077?q=%7B%22search%22%3A%5B%22the+Password+Protection+Act+of+2013%22%5D%7D>; *see also* Password Protection Act of 2013 S. 1426, 113th<sup>th</sup> Con. , (2013), available at <http://beta.congress.gov/bill/113th-congress/senate-bill/1426?q=%7B%22search%22%3A%5B%22the+Password+Protection+Act+of+2013%22%5D%7D>

146. *See* H.R. 537; H.R. 2077; *see also* *Employer Access to Social Media Usernames and Passwords*, *supra* note 142.

147. *See* H.R. 537. It has drawn seven co-sponsors. *Id.* *See* H.R. 2077. It has drawn thirty-nine House co-sponsors. *Id.* The Senate version has six co-sponsors. S. 1426.

148. *See* Melissa Gillepsie, *Using Social Media for Recruiting: You Can't Unring the Bell*, HR KNOWLEDGE (July 14, 2014), <http://www.hrknowledge.com/social-media-recruiting-cant-unring-the-bell/>

protected class information to discriminate in hiring, the employer will have intentionally violated the relevant federal and state statutes. Social media often provides information enabling direct discrimination that a résumé or even interviews do not provide. A candidate's religion, national origin, lineage, marital status, number and age of children, spouse's job, height and weight, organizations a candidate belongs to, sex, age, and disability are among factors that federal acts prohibit discrimination based upon and which may be available through social media.<sup>149</sup> A sample examination of a U.S. Senator's Facebook site and Wikipedia site reveal his religion, race, marital status, number of children, approximate height and weight from photos, organizations he belongs to, exact date of birth/age, and even his parents' names.<sup>150</sup> Many other Americans are similarly transparent in social media and vulnerable to discrimination prohibited by Title VII, the ADA, and the ADEA.

### B. Disparate Impact

Most employers will not intend to discriminate against candidates based on a protected class. Yet an employer *not motivated by discriminatory intent* may still run afoul of federal and state protections when its hiring practices utilize social media. An organization's social media-informed employment decisions may disparately impact a protected class candidate. For example, an employer disapproving of or disliking "rap music" may tend to assign a low rating to or pass over applicants with "Likes" and links to "gangsta rap" artists. These candidates may disproportionately represent African American men. An employer may disapprove of candidates who "Like" Jimmy Buffet or the Rolling Stones and may disproportionately impact applicants over fifty years of age. An employer may disapprove of candidates who "Like" the Susan G. Komen Foundation or a religious figure such as Pope Francis or the Dalai Lama and impact candidates of particular religions.

The United States Supreme Court in *Griggs v. Duke Power Co.*, enunciated that Title VII

---

bell/.

149. See *Prohibited Employment Policies/Practices*, *supra* note 50.

150. See, e.g., U.S. Senator Dean Heller, FACEBOOK, [https://www.facebook.com/SenDeanHeller/info?ref=page\\_internal](https://www.facebook.com/SenDeanHeller/info?ref=page_internal) (last visited Sept. 13, 2014); Dean Heller, WIKIPEDIA, [http://en.wikipedia.org/w/index.php?title=Dean\\_Heller&oldid=625288842](http://en.wikipedia.org/w/index.php?title=Dean_Heller&oldid=625288842) (last visited Sept. 13, 2014).

proscribes not only overt discrimination but also practices that are fair in form, but discriminatory in operation. The touchstone is business necessity . . . . [G]ood intent or absence of discriminatory intent does not redeem employment procedures or testing mechanisms that operate as “built-in headwinds” for minority groups and are unrelated to measuring job capability.<sup>151</sup>

Allocation of proof in disparate impact cases first falls on the plaintiff to prove that the challenged practice or selection device has a substantial adverse impact on the basis of race, color, religion, sex, or national origin.<sup>152</sup> The defendant may attack the statistical analysis or offer differing statistics.<sup>153</sup> If the plaintiff establishes a statistical disparate impact, the employer must defend practice and prove that it is job-related for the position in question and consistent with business necessity.<sup>154</sup> A plaintiff may also prevail even if the employer proves business necessity, if the plaintiff can show the employer has refused to adopt an alternative employment practice that would satisfy the employer’s legitimate interests without having a disparate impact on a protected class.<sup>155</sup> State acts and judicial decision mirror the federal framework.

Therefore, an employer whose hiring practices produce statistical evidence of disparate impact potentially faces litigation and the burden of proving business necessity for the practice as well as the need to prove that it could not adopt an alternative employment practice that would not have a disparate impact on a protected class. An employer using screening of social media as part of the hiring process should proceed with these needs in mind.

## VII. LIFE STYLE DISCRIMINATION STATUTES

Much of the information shared on personal social media sites

---

151. *Griggs v. Duke Power Co.*, 401 U.S. 424, 431-32 (1971). In 1989, the Supreme Court reduced the defendant’s burden of business necessity to a burden of producing evidence of business justification. See *Wards Cove Packing Co. v. Antonio*, 490 U.S. 642, 6578 (1989). The Civil Rights Act of 1991 overturned that portion of the *Wards Cove* decision. *EEO: Disparate Impact*, HR-GUIDE.COM, <http://www.hr-guide.com/data/G702.htm> (last visited Sept. 28, 2014); see also *The Civil Rights Act of 1991*, EEOC, <http://www.eeoc.gov/eeoc/history/35th/1990s/civilrights.html> (last visited Jan. 9, 2015).

152. See 42 U.S.C. § 2000e-2(k)(1)(A)(i) (2006).

153. See *Guinard v. City of New York*, 800 F. Supp. 1083, 1088 (E.D.N.Y. 1992) (“A *prima facie* case of disparate impact can be established by showing either ‘a gross statistical disparity’ or ‘statistically significant adverse impact coupled with other evidence of discrimination.’”).

154. See 42 U.S.C. § 2000e-2(k)(1)(B)(ii).

155. See *id.* § 2000e-2(k)(1)(A)(ii).

provides a very transparent look at a person's "life style" – exposing many activities that a person engages in – truly the "good, the bad, and the ugly. In the 1990s, well before the emergence of social media, legislatures in several states passed "life style" discrimination statutes which prevent employers from discriminating against employees due to their legal, but perhaps controversial life style choices.<sup>156</sup> Nine of these "Life Style" statutes apply to discrimination against job applicants as well as employees.<sup>157</sup>

"Life style" discrimination statutes have taken one of two forms in varying states.<sup>158</sup> Lawful Product Statutes make it "unlawful for an employer to treat an employee or applicant less favorably because of the individual's off-duty, off-premises use of any lawful product or lawful consumable product."<sup>159</sup> These statutes have been adopted in six states: Illinois, Minnesota, Montana, Nevada, North Carolina, and Wisconsin.<sup>160</sup> Four states have enacted Lawful Activity Statutes that make it "unlawful for an employer to treat an employee [or applicant] less favorably because of any lawful activity in which the individual participates while off-duty and away from the worksite."<sup>161</sup> These are California, Colorado, New York, and North Dakota.<sup>162</sup>

"Lawful products" statutes, in theory, include a very broad scope of products including alcohol, tobacco, firearms, or pornography by adults of legal age.<sup>163</sup> The use of these controversial products or products that might put an employee at physical risk such as skydiving, riding motorcycles or snowmobiles is protected.<sup>164</sup> "Lawful activities" may encompass a larger scope of protections. Thus, in these nine states, if an employer finds photos of potential employees on social media sites using legal products or engaged in legal activities that might be perceived as demonstrating a lack of judgment, lack of organizational fit, physically risky, or otherwise distasteful, and makes a detrimental decision in hiring based on this information, the employer may violate state law.

---

156. See Robert M. Howie & Laurence A. Shapero, *Lifestyle Discrimination Statutes: A Dangerous Erosion of At-Will Employment, a Passing Fad, or Both?* 31 EMP. REL. L. J. 21, 21 (2005).

157. See *id.* at 22.

158. *Id.*

159. *Id.*

160. See Nat'l Conference of State Legislatures, *Discrimination Regarding Off-Duty Conduct*, [www.ncsl.org/documents/employ/off-dutyconductdiscrimination.pdf](http://www.ncsl.org/documents/employ/off-dutyconductdiscrimination.pdf) (last updated Oct. 18, 2010).

161. Howie & Laurence, *supra* note 156, at 22.

162. See Nat'l Conference of State Legislatures, *supra* note 160.

163. See Howie & Laurence, *supra* note 156, at 23-28.

164. See *id.* at 25.

Remedies vary by state.<sup>165</sup>

In addition to broad-brush state statutes encompassing many activities and products, use of a specific lawful product has been singled out for protection. According to the National Conference of State Legislatures, eighteen states and the District of Columbia have enacted statutes that make it unlawful to discriminate in hiring decisions against persons who lawfully use tobacco products.<sup>166</sup> Thus, an employer who learns of an applicant's tobacco use through social media and uses that as a factor in hiring may violate state law.

Few recorded cases exist testing the effect of these statutes and none have yet involved social media. Employer advocates question the effect of statutes due to their "unnecessary intrusions of the at-will employment relationship without a significant corresponding policy benefit."<sup>167</sup> Other authors argue that courts have rendered life style statutes meaningless and specific legislation should be enacted by either the federal government or the states to restrict employer actions based on electronic communications.<sup>168</sup> Employers in states with life style statutes must be aware of their scope and potential impact in selecting potential employees and must be aware that legal activities identified through social media research may be protected from employment discrimination.

#### VIII. RECORD KEEPING RESPONSIBILITIES

Both the federal government and state governments require employers to retain records used in employment searches and hiring.<sup>169</sup> All application forms and records dealing with hiring must be retained by private employers for one year from the date of making the record or of the personnel action involved, whichever occurs later.<sup>170</sup> Educational institutions, state, and local governments must retain such records for two years from the date of making the record or the personnel action

---

165. See, e.g., *id.* at 28 (stating that Colorado's Lawful Activity Statute requires the court to award the prevailing party court costs and reasonable attorney's fees).

166. See Nat'l Conference of State Legislatures, *supra* note 160 (including Connecticut, District of Columbia, Indiana, Kentucky, Louisiana, Maine, Mississippi, Missouri, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, South Carolina, South Dakota, Virginia, West Virginia, Wisconsin, and Wyoming).

167. See Howie & Laurence, *supra* note 156, at 22.

168. See Joseph Lipps, *State Lifestyle Statutes and the Blogosphere: Autonomy for Private Employees in the Internet Age*, 72 OHIO ST. L.J. 645, 675-77 (2011).

169. See, e.g., 42 U.S.C. § 2000e-8(c) (2006); 13 TEX. ADMIN. CODE § 6.10 (2012).

170. See 29 C.F.R. § 1602.14 (2013).

whichever occurs later.<sup>171</sup> When a charge of discrimination has been filed under Title VII or the ADA, records must be retained until final resolution of the charge or action.<sup>172</sup> The law firm Constangy, Brooks & Smith, LLP, publishes an outline of federal record-keeping requirements and recommends retaining applications, résumés, job advertisements, and other key documents related to hiring generally for four years.<sup>173</sup> These federal requirements appear to mandate the keeping of records in reviewing social media websites and in retaining the information viewed.<sup>174</sup> State statutes are typically similar.<sup>175</sup> Screen shots and other technical tools allow capture and retention.

Employers who make decisions based on negative information found via searches of social media sites clearly need to document what information was found and why this impacted the hiring decision.<sup>176</sup> An employer needs to be able to demonstrate that if social media searches were used in the employment process that decisions were made based on permissible and relevant information. Employers should retain computer screen shots of materials legitimately relevant to decision making as part of the search file.

## IX. FAIR CREDIT REPORTING ACT

In an opinion letter dated May 9, 2011, the Federal Trade Commission (FTC) characterized a company providing employers with an “[i]nternet and social media background screening service” as a consumer reporting agency.<sup>177</sup> The FTC stated that “[c]onsumer reporting agencies must comply with several different [Fair Credit Reporting Act] provisions, and these compliance obligations apply equally in the social networking context.”<sup>178</sup>

171. 29 C.F.R. §§ 1602.31, .40, .49 (2010).

172. 29 C.F.R. § 1602.14.

173. See Constangy, Brooks & Smith, LLP, *Outline of Federal Employment Law Record Keeping Requirements*, [http://www.constangy.com/media/materials/42\\_Federal%20Recordkeeping%20Chart%202011.pdf](http://www.constangy.com/media/materials/42_Federal%20Recordkeeping%20Chart%202011.pdf) (last visited February 9, 2014).

174. See *id.*

175. See, e.g., 13 TEX. ADMIN. CODE § 6.10 (2012).

176. See *supra* text accompanying notes 171-73.

177. Letter from Maneesha Mithal, Associate Dir., FTC, to Renee Jackson, Esquire, Nixon Peabody LLP (May 9, 2011), (on file with FTC), available at [http://www.ftc.gov/sites/default/files/documents/closing\\_letters/social-intelligence-corporation/110509socialintelligenceletter.pdf](http://www.ftc.gov/sites/default/files/documents/closing_letters/social-intelligence-corporation/110509socialintelligenceletter.pdf).

178. *Id.*

The federal Fair Credit Reporting Act<sup>179</sup> applies to any employer using a third party to conduct inquiries about potential employees.<sup>180</sup> The Act provides that a person may not procure a report for employment purposes “unless (i) a clear and conspicuous disclosure has been made in writing to the consumer . . . before the report is procured . . . and (ii) the consumer has authorized [this procurement] in writing.”<sup>181</sup> It authorizes a consumer reporting agency to provide a report for employment purposes only if the person who obtains the report certifies to the agency that the consumer has been provided a disclosure, has authorized the report and that the report will not be used in violation of any federal or state equal opportunity law or regulation.<sup>182</sup> The Act requires that before using a consumer report for employment purposes for adverse actions, “the person intending to take such adverse action shall provide to the consumer to whom the report relates – (i) a copy of the report; and (ii) a description in writing of the rights of the consumer under this subchapter, as prescribed. . . .”<sup>183</sup>

Employers outsourcing the process should seek legally compliant third-party service providers. Providers are adapting and filling this market niche.<sup>184</sup>

## X. EMPLOYER STRATEGIES

How should an employer approach use of searching social media sites to screen employee applicants? First, the employer must make a conscious decision as to whether to employ this tool and likewise either establish a policy prohibiting use or one that provides a uniform approach for screening social networking websites.<sup>185</sup> A legitimate business rationale for using social media should be documented.

---

179. 15 U.S.C. § 1681 (2012).

180. *See id.* § 1681a(d)(2)(C).

181. *Id.* § 1681b(b)(2)(A)(i)-(ii).

182. *See id.* § 1681b(b)(1).

183. *Id.* § 1681b(b)(3)(A).

184. *See, e.g., About, SOCIAL INTELLIGENCE*, <http://socialintel.com/company/about.html> (last visited Sept. 13, 2014). Social Intelligence “provides social media data, tools, and reports to commercial and Government organizations.” *Id.* The company advertises on its website that it “adheres to the guidelines of the Fair Credit Reporting Act (FCRA) and is compliant with Federal and State law.” *Id.* It uses pre-defined filters to assure that any criteria used are guaranteed to be relevant to the job and it redacts federal and state protected class information. *See FAQs, SOCIAL INTELLIGENCE*, <http://socialintel.com/faqs.html> (last visited Sept. 28, 2014).

185. Renee L. Warning & F. Robert Buchanaan, *Social Networking Web Sites: The Legal and Ethical Aspects of Pre-Employment Screening and Employee Surveillance*, 4 J. OF HUM. RESOURCES EDUC. (2010).

Employer research of social networking sites should be conducted methodically to ensure consistency across all legally-protected classes. Employers should document the search process and findings and preserve these findings as part of the search record.

Specific advice to employers include the following:

- Give notice to the job applicant and obtain written approval before searching.
- Do not seek answers to questions that your organization would not ask in an interview.
- Make sure that the social media profile is that of the applicant.
- Give applicants the opportunity to clarify information posted in order to insure that it is not incorrect or faked. If a third party has provided the report upon which adverse action is to be taken, the applicant must be notified and provided the report in compliance with the Fair Credit Reporting Act.
- Do not ask applicants for passwords to profiles. Asking or requiring passwords is viewed as extremely intrusive of privacy. This action may violate the federal Stored Communications Act<sup>186</sup> and may violate state statutes.
- Both policy and practice should prohibit use of protected class information revealed in searches.
- Factors that have a disproportionate impact on a protected class should not be used in decision making unless they have relevance to the position. A permissible factor might be identifying drug activity due to its impact on safety and absenteeism in the workplace—even if this factor inadvertently affects males than females. A person other than the decision maker should conduct reviews of social media sites and search for specified information, collect and maintain it in a uniform manner. This ensures that the decision maker is not exposed to information that would be inappropriate to use in the hiring decision. It may be quite relevant for the decision maker to know that an applicant is featured

---

186. 18 U.S.C. §§ 2701–2712 (2012).

smoking marijuana or exposing himself, is a “Friend” of a racist organization, or has complained publically about his current employer. It is not relevant for the decision maker to know protected class information.

- Federal and state record keeping requirements need to be satisfied. Means of capture and retention of information from the profiles of candidates need to be established and complied with.

## XI. CONCLUSION

A significant percentage of American employers are screening job applicants’ social media as part of their hiring process. Membership in social media websites such as Facebook includes a substantial portion of the American pool of job applicants.<sup>187</sup> Search engines and search tools within social media websites allow rapid search for information about applicants, revealing substantial amounts of potentially *relevant* and *protected class* information alike.<sup>188</sup> Some of the information available from social networking sites may be highly valuable and relevant in selecting successful candidates. Use of other information may violate federal and state acts against employment discrimination when information is used to directly discriminate or if the use disproportionately impacts protected classes of potential employees. Requests for passwords from applicants may violate state and federal statutes. Even using social media to avoid hiring employees who engage in risky, but legal behaviors may contravene laws in several states. Employers who use social media in hiring should do so methodically to avoid discrimination and have policies in place guiding its uniform execution and record retention.

---

187. See Christina Wilkie, ‘Job Seekers’ Make 75 Percent of U.S. Workforce, Survey Finds, HUFF POST MONEY (Oct. 9, 2012, 7:08 PM), [http://www.huffingtonpost.com/2012/10/09/job-seekers-jobvite-survey\\_n\\_1952727.html](http://www.huffingtonpost.com/2012/10/09/job-seekers-jobvite-survey_n_1952727.html).

188. See Lisa Quast, *Recruiting, Reinvented: How Companies Are Using Social Media in the Hiring Process*, FORBES (May 5, 2012, 9:30 AM), <http://www.forbes.com/sites/lisaquast/2012/05/21/recruiting-reinvented-how-companies-are-using-social-media-in-the-hiring-process/>. NS 21, 1.2(a), 2.1(c), 15.1(d), 8(a), 8(b), 18.2.2(b), 18.2.2(b)(i)(3), 18.2.2(c), 18.2.2(d).

