

2008

## Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants

Ian Byrnside

Follow this and additional works at: <https://scholarship.law.vanderbilt.edu/jetlaw>



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

---

### Recommended Citation

Ian Byrnside, Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants, 10 *Vanderbilt Journal of Entertainment and Technology Law* 445 (2020)  
Available at: <https://scholarship.law.vanderbilt.edu/jetlaw/vol10/iss2/5>

This Note is brought to you for free and open access by Scholarship@Vanderbilt Law. It has been accepted for inclusion in Vanderbilt Journal of Entertainment & Technology Law by an authorized editor of Scholarship@Vanderbilt Law. For more information, please contact [mark.j.williams@vanderbilt.edu](mailto:mark.j.williams@vanderbilt.edu).

# Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants

## ABSTRACT

*As social networking sites like Facebook.com and MySpace.com continue to grow in popularity, college students and other job applicants voluntarily divulge an increasing amount of personal information on them, often unaware of the potential negative effects it may have on their search for employment. Employers are beginning to take note of this trend and are increasingly using applicants' social networking profiles to supplement traditional application information. Many applicants feel that employers should not base employment decisions on social networking profiles in any way and believe that it is illegal for employers to do so. Yet, it appears that employers that view this information are on safe legal ground for now. The use of such social networking sites for gathering applicant information raises several potential legal issues, including invasion of privacy, discrimination, violation of the Fair Credit Reporting Act, violation of terms of service, and defamation. While some of these claims may seem unlikely to succeed and difficult to prove, this is an emerging area of law that is far from settled. This note will provide several suggestions for successfully navigating social networking sites in the employment relationship for applicants and employers alike.*

## TABLE OF CONTENTS

I.	HISTORY CONCERNING THE LEGALITY OF EMPLOYERS' INFORMATION-GATHERING TECHNIQUES.....	448
II.	INTRODUCTION TO SOCIAL NETWORKING SITES .....	453
	A. <i>The Rise and Popularity of MySpace and Facebook</i> .....	454
	B. <i>Applicants Under Investigation</i> .....	456
III.	POTENTIAL LEGAL ISSUES ARISING FROM EMPLOYER INVESTIGATION OF APPLICANTS' SOCIAL NETWORKING PROFILES.....	458

A. <i>Invasion of Privacy</i> .....	459
B. <i>Discrimination</i> .....	462
C. <i>Fair Credit Reporting Act</i> .....	465
D. <i>Violation of Terms of Service</i> .....	466
E. <i>Defamation</i> .....	468
IV. POTENTIAL PITFALLS OF EMPLOYERS' INVESTIGATION OF APPLICANTS' SOCIAL NETWORKING PROFILES .....	469
A. <i>Problem of Too Much Information</i> .....	469
B. <i>Issues Concerning Identity and Authenticity</i> .....	470
V. SOLUTION AND RECOMMENDATIONS FOR THE FUTURE .....	472
A. <i>Suggestions for Applicants</i> .....	473
B. <i>Suggestions for Employers</i> .....	474
VI. CONCLUSION .....	476

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.<sup>1</sup>

- Brad Karsh, President, JobBound

Social networking sites, such as MySpace.com and Facebook.com, have experienced ever-increasing popularity over the past few years, with users divulging more and more personal information on them. These sites allow users to post a variety of information, including photographs, journal entries, personal interests, and a myriad of other personal information. While some users post innocent information, such as their favorite bands or their favorite movies, others include more obscene listings, such as "I buried a hooker in the woods behind Sandburg Halls[,] I enjoy sex[, and] I'm a pothead and proud of it."<sup>2</sup> College students and other potential job applicants may see this information as a joke to be viewed only by their friends. However, prospective employers are becoming increasingly aware of these sites and are taking advantage of the

---

1. Press Release, CollegeGrad.com, MySpace is Public Space When it Comes to Job Search; Entry Level Job Seekers – It's Time to Reconsider the Web (July 26, 2006), <http://www.collegegrad.com/press/myspace.shtml>.

2. Joe Ahlers, *Facebook, MySpace Raise Security Concerns for College Students*, LEADER, May 10, 2006, <http://media.www.uwmleader.com/media/storage/paper980/news/2006/05/10/Beat/Facebook.Myspace.Raise.Security.Concerns.For.College.Students-2043673.shtml>.

massive amount of newly available information to assist them in their hiring decisions.

One Duke University student found out about this recent phenomenon the hard way. Ana Homayoun, the manager of a small educational consulting firm in San Francisco, visited Duke University in the spring of 2006 to interview a potential job applicant.<sup>3</sup> Before interviewing her, however, Homayoun decided to look at the applicant's Facebook page.<sup>4</sup> There she found "explicit photographs and commentary about the student's sexual escapades, drinking and pot smoking, including testimonials from friends," in addition to pictures of the applicant "passed out after drinking."<sup>5</sup> "When I saw that, I thought, 'O.K., so much for that,'" said Homayoun.<sup>6</sup>

Unfortunately, this type of social networking profile is not uncommon. A glance at one University of Texas at San Antonio student's online profile reveals that his college minor is "beer drinking," and the profile "includes pictures of himself sloshed and partying with inebriated friends."<sup>7</sup> Similarly, a Texas State University student's profile lists "the rules of phoning people when you are drunk. Rule No. 11: 'Drunk dialing should be fun and light-hearted or dirty and sex-crazed.'"<sup>8</sup> Are these the type of people that a professional employer would want to hire? Many employers who discovered similar profiles for job applicants do not think so.<sup>9</sup>

As social networking sites become more and more commonplace in today's society, there is increasing attention being given to reports of employers rejecting applicants or firing employees based on information discovered on these sites.<sup>10</sup> Although employers have begun using social networking sites to assist with hiring decisions, the potential legal ramifications of such a practice are unclear, to say the least. No case has been brought on the basis of such a use of these social networking sites. However, the increasing popularity of such sites brings with it the potential for numerous legal problems to arise

---

3. See Alan Finder, *When a Risque Online Persona Undermines a Chance for a Job*, N.Y. TIMES, June 11, 2006, at 1.

4. *Id.*

5. *Id.*

6. *Id.*

7. Ken Rodriguez, *Want a Job After Graduation? Don't Reveal Your Wild Side Online*, SAN ANTONIO EXPRESS-NEWS, July 5, 2006, at 3A.

8. *Id.*

9. See Finder, *supra* note 3, at 1.

10. George's Employment Blawg, *Employers Using Facebook for Background Checking, Part I*, [http://www.collegerecruiter.com/weblog/archives/2006/09/employers\\_using.php](http://www.collegerecruiter.com/weblog/archives/2006/09/employers_using.php) (Dec. 5, 2006, 17:33 PST) [hereinafter *Employers Using Facebook Part I*]; see *infra* Part II.B (providing examples of employers use of social networking sites).

in this “emerging area of law,” bolstering the chance that such a case may arise in the not-so-distant future.<sup>11</sup>

This note will begin with a brief history of employers’ information-gathering techniques regarding applicants and will discuss the emergence of social networking sites in mainstream culture. This note will then address the potential legal concerns that the use of such sites could have in the employment field. Finally, this note will propose a solution to the problem created by the competing interests of individuals desiring freedom of expression and employers desiring quality employees, and will provide advice for applicants and employers regarding the use of social networking sites.

## I. HISTORY CONCERNING THE LEGALITY OF EMPLOYERS’ INFORMATION-GATHERING TECHNIQUES

Employers often seek as much information as possible about job applicants to ensure the best fit between an applicant and the employer’s organization.<sup>12</sup> In order to obtain such information, employers have utilized a vast number of information-gathering techniques; the techniques employed depend largely on the position to be filled.<sup>13</sup> Ultimately, employers seek employees with characteristics that will maximize work productivity and minimize costs and liability.<sup>14</sup>

Over the past few years, in an effort to increase the productivity of their work forces and decrease their potential liability, employers have begun gathering an increasing amount of information about applicants through various new sources.<sup>15</sup> Historically, employment pre-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>16</sup> Employers are generally permitted to investigate

---

11. *Hiring: Pitfalls of Checking Job Applicants’ Personal Web Pages*, MANAGING ACCOUNTS PAYABLE, Oct. 2006, at 4, 5 [hereinafter *Hiring: Pitfalls*] (quoting Chris Wolf, Partner, Proskauer Rose LLP).

12. 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).

13. See *id.* at 368.

14. See *id.* at 367.

15. See *id.* at 369.

16. See generally 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, 255-261 (1994) (outlining traditional methods of pre-employment screening).

applicants and employees; however, several legal concerns arising from these investigations have become a major focus of recent legislation and litigation.<sup>17</sup> While many of the aforementioned techniques are generally considered to be legal methods of investigation for employers, they may raise issues of discrimination under Title VII of the Civil Rights Act of 1964 (Title VII) and the Americans with Disabilities Act (the ADA).<sup>18</sup>

Title VII is the primary federal anti-discrimination statute.<sup>19</sup> It prohibits employers from discriminating against applicants and employees "because of such individual's race, color, religion, sex, or national origin."<sup>20</sup> However, Title VII does not prohibit employment decisions or actions that stem from legitimate, non-discriminatory motives. While most courts have held that, under Title VII, employers may ask "questions that elicit information concerning protected class status," so long as the information is not used in the decision-making process, such questions may suggest discrimination or a discriminatory intent.<sup>21</sup> Furthermore, asking such questions may make it difficult to prove that discrimination was not involved in the decision-making process. Therefore, the Equal Employment Opportunity Commission's (EEOC) Guide to Pre-Employment Inquiries advises against asking questions directly concerning protected class status and neutral questions that may have a disparate impact on members of a protected class, as such questions could provide "evidence of discrimination prohibited by Title VII."<sup>22</sup> The EEOC Guide explains that employment decisions based upon such questions violate Title VII "unless the information is needed to judge an applicant's competence or qualification for the job in question."<sup>23</sup>

Similarly, the ADA prohibits discrimination in employment decisions against "an individual with a disability who, with or without reasonable accommodation, can perform the essential functions of the employment position that such individual holds or desires."<sup>24</sup>

---

17. See *id.* at 254 (noting that "where the employers' rights end and the employees' privacy rights begin" is a key issue behind current litigation).

18. See Befort, *supra* note 12, at 381. See generally Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e to 2000e-17 (2000); Americans with Disabilities Act, 42 U.S.C. §§ 12111-12117 (2000).

19. Befort, *supra* note 12, at 381.

20. 42 U.S.C. § 2000e-2.

21. Befort, *supra* note 12, at 381 (citing *Bruno v. City of Crown Point*, 950 F.2d 355, 363-65 (7th Cir. 1991)).

22. *Id.* at 382.

23. *Id.*

24. 42 U.S.C. § 12111(8).

However, while the ADA prohibits employers from asking applicants about the existence or nature of disabilities they may have, it does permit employers to inquire as to the ability of applicants to perform job-related functions.<sup>25</sup> The EEOC claims that this prohibition “helps ensure that an applicant’s possible hidden disability (including a prior history of a disability) is not considered before the employer evaluates an applicant’s non-medical qualifications.”<sup>26</sup> According to the EEOC, employers may not ask applicants any disability-related questions or any questions indirectly related to an applicant’s disability status.<sup>27</sup> Therefore, employers asking questions related to disabilities may be in violation of the ADA even if such information is not used in the decision-making process.<sup>28</sup>

Employers conducting background checks of applicants have also faced several legal issues.<sup>29</sup> Employers often check applicants’ criminal records. However, such practice is not illegal, so long as employment decisions based on this information are consistent with “business necessity” and do not have a disparate impact on a certain class of applicants.<sup>30</sup> While there is no federal statute limiting employer investigation of an applicant’s criminal or conviction records, forty-one states have prohibited the use of arrest records, and therefore, courts are more likely to accept decisions made based upon conviction records, as opposed to decisions made based upon arrest records.<sup>31</sup>

Similarly, employers conducting credit reports on applicants have certain legal obligations. Under the Fair Credit Reporting Act (FCRA),<sup>32</sup> employers may not obtain credit reports of applicants without first obtaining the individual’s consent.<sup>33</sup> The FCRA requires an employer to “clearly and accurately” notify applicants in writing if they will be the subject of a consumer credit report prepared by a

25. See 42 U.S.C. § 12112(d)(2).

26. EQUAL EMPLOYMENT OPPORTUNITY COMM’N, NOTICE NO. 915.002, ADA ENFORCEMENT GUIDANCE: PREEMPLOYMENT DISABILITY-RELATED QUESTIONS AND MEDICAL EXAMINATIONS 1 (1995) [hereinafter EEOC GUIDANCE].

27. See Befort, *supra* note 12, at 383.

28. See *id.*

29. See *id.* at 366.

30. See *id.* at 404-05.

31. See *id.* (rationalizing that “conviction records are more reliable . . . because the criminal justice system has established that misconduct actually occurred”). Furthermore, a majority of states restrict or prohibit an employer’s use of arrest records, reflecting a similar concern that the lack of established guilt is discriminatory. See Ecker, *supra* note 16, at 255-56.

32. 15 U.S.C. §§ 1681-1681t (2000 & Supp. 2003).

33. See Ecker, *supra* note 16, at 258.

consumer reporting agency.”<sup>34</sup> Applicants must also be given notice if a credit report was used in making an unfavorable hiring decision.<sup>35</sup> Furthermore, employers may not base hiring decisions solely on the results of credit reports and may be held liable if decisions based on these reports have a disparate impact on a protected class.<sup>36</sup>

Some of the most controversial techniques employers use to investigate applicants involve various examinations, including polygraph tests. Since the enactment of the Employee Polygraph Protection Act of 1988 (EPPA),<sup>37</sup> private employers have been effectively banned from requiring applicants to submit to polygraph tests.<sup>38</sup> The EPPA prohibits employers from asking applicants to take polygraph tests or using the results of polygraph tests in making employment decisions.<sup>39</sup> Similarly, honesty, personality, and other ability tests have proven problematic for employers.<sup>40</sup> Although these tests remain largely unregulated and are generally permissible tools for employers to use in investigating applicants, privacy, reliability, and discriminatory concerns often arise.<sup>41</sup>

Employers also often use medical examinations and drug tests in the hiring process. The ADA prohibits employers from requiring applicants to submit to medical examinations.<sup>42</sup> However, employers may require a medical examination “after making an offer of employment that is conditional upon the satisfactory outcome of the examination, if it is required of all new hires within the same job category.”<sup>43</sup> Generally, the ADA permits medical examinations after an offer of employment has been extended, so long as “any disability-related criteria used to screen out a prospective employee [is] ‘job-related and consistent with business necessity.’”<sup>44</sup>

Unlike medical testing, drug testing of applicants is generally permissible so long as it is uniformly administered to all applicants.<sup>45</sup>

---

34. Befort, *supra* note 12, at 406 (quoting 15 U.S.C. § 1681d (1994)).

35. *See id.* (citing 15 U.S.C. § 1681m).

36. *See id.*; *cf.* 11 U.S.C. § 525(b) (2000) (stating that, under the Bankruptcy Act, a private employer may not terminate an employee solely because he is a debtor or because he is bankrupt).

37. 29 U.S.C. §§ 2001-2009 (2000).

38. *See* Befort, *supra* note 12, at 402.

39. *Id.*; *see* 29 U.S.C. § 2002.

40. *See* Ecker, *supra* note 16, at 260 (explaining that subjective tests “attempt to measure intangible qualities” and lead to “inconsistent and unreliable results”).

41. Befort, *supra* note 12, at 403.

42. 42 U.S.C. § 12112(d)(2) (2000).

43. Befort, *supra* note 12, at 386.

44. *Id.* at 386-387 (quoting 42 U.S.C. § 12112(d)(4)).

45. Ecker, *supra* note 16, at 261.



Courts have generally allowed such testing, despite applicant claims of invasion of privacy, because the testing is typically performed with the applicant's knowledge and consent as a condition of employment.<sup>46</sup> The ADA also supports the general permissibility of drug testing for applicants, as it "expressly states that [drug] testing . . . is not a 'medical examination' and is not restricted by the ADA."<sup>47</sup> However, the ADA does not view alcohol testing in the same way as drug testing, likening alcohol testing to a medical examination.<sup>48</sup>

Underlying all of these concerns is the applicant's interest in retaining his or her right to privacy. One of the most common concerns among applicants is that employer investigations will invade their right to privacy and will reveal information that they believe should not be used in the decision-making process.<sup>49</sup> Privacy in the workplace has been an increasingly prominent area of legal discussion, particularly with respect to the off-duty activity of applicants, which applicants strongly believe should not be the prospective employer's concern.<sup>50</sup> Applicants rely on several theories of privacy to claim that employers should not be able to trespass into their private lives; primarily, applicants rely on tort law in bringing claims, based on the belief that they have a right to do things in private, particularly if they are off the employer's premises.<sup>51</sup> Applicants also look to the Fourth Amendment of the U.S. Constitution, alleging that employer investigation into their private lives constitutes an illegal search and invades their right to free space.<sup>52</sup>

However, claims of invasion of privacy require that the claimant have a *reasonable* expectation of privacy.<sup>53</sup> Applicants are not always aware of this requirement and often seek the ability to control their off-duty conduct regardless of a reasonable expectation of privacy.<sup>54</sup> Applicants believe that what they do off the job "should be of no concern to their employer" and should not be a factor in

---

46. See *id.*

47. Befort, *supra* note 12, at 392 (quoting 42 U.S.C. § 12114(d)(1) (1994)).

48. See *id.*

49. See Ecker, *supra* note 16, at 274.

50. See, e.g., Stephen D. Sugarman, "Lifestyle" Discrimination in Employment, 24 BERKELEY J. EMP. & LAB. L. 377, 378, 407 (2003) (discussing the effects that methods of collecting information about employee's off-duty conduct has on their privacy rights).

51. See *id.* at 402-03.

52. See *id.* at 403-06.

53. See *California v. Greenwood*, 486 U.S. 35, 39-40 (1988).

54. See Sugarman, *supra* note 50, at 380.

employment decisions.<sup>55</sup> They want to partake in off-duty conduct without fear of suffering possible negative consequences at the hands of their employers as a result of such conduct.<sup>56</sup> Essentially, applicants are seeking “a notion of personal autonomy or self-identity.”<sup>57</sup>

As privacy concerns become increasingly important, technological advances, such as social networking sites, are constantly making it easier for employers to obtain information about applicants and employees.<sup>58</sup> “[T]he more economical it becomes to obtain information about a potential employee’s private life, the greater the likelihood employers will use it.”<sup>59</sup> As the use of social networking sites as an information-gathering technique increases, numerous legal and ethical concerns are likely to arise.

## II. INTRODUCTION TO SOCIAL NETWORKING SITES

Like so many modern technological advancements, social networking sites exploded in popularity in an extremely short time-span. Social networking sites are virtual communities on the Internet where people may go to find and “connect with others who have similar interests.”<sup>60</sup> Hundreds of social networking sites exist.<sup>61</sup> While these sites differ in many ways, they generally consist of a personal website (often called a profile) with photographs and text, including the user’s picture, likes and dislikes, interests, blog entries, geographic location, gender, links to the profiles of other friends on the site, and various other types of information.<sup>62</sup> Many of these sites also include an array of personal information, such as the user’s name, address, telephone number, and e-mail address, and offer varying degrees of privacy controls to allow users to restrict access to their

---

55. *Id.*

56. *Id.* at 406.

57. *Id.*

58. *See* Befort, *supra* note 12, at 370-71.

59. Gail L. Heriot, *The New Feudalism: The Unintended Destination of Contemporary Trends in Employment Law*, 28 GA. L. REV. 167, 173 n.18 (1993).

60. Cyber Safety Glossary, Definition of Social Networking Sites, [http://www.bsacybersafety.com/threat/social\\_networking.cfm](http://www.bsacybersafety.com/threat/social_networking.cfm) (last visited Oct. 25, 2007).

61. *Id.*

62. *See* Cyber Safety Glossary, *supra* note 60; STUDENT LEGAL SERVICES, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, MYSPACE MAY NOT BE JUST YOUR SPACE: WHAT EMPLOYERS FIND ON THE INTERNET MAY HURT YOU, <http://www.odos.uiuc.edu/sls/pdfbrochures/myspacedotcom.pdf> (last visited Oct. 27, 2007).

profiles.<sup>63</sup> Social networking sites are especially popular among teenagers and young adults as a method for meeting new people,<sup>64</sup> keeping in touch with friends, and generally “communicat[ing] with each other about anything and everything.”<sup>65</sup> Two of the most popular social networking sites, MySpace.com (MySpace) and Facebook.com (Facebook),<sup>66</sup> are the focus of this note.

### A. *The Rise and Popularity of MySpace and Facebook*

MySpace and Facebook, created just five years and four years ago, respectively, have already amassed millions of users and reached astounding popularity among Internet users.<sup>67</sup> MySpace is the most popular social networking site in the United States, racking up over 1 billion page views per day and having 100 million registered users, with 56 million unique visitors each month.<sup>68</sup> Similarly, in its first four years of existence, Facebook has topped the Internet charts with over 54 billion page views per month and over 47 million registered

63. See Cyber Safety Glossary, *supra* note 60; STUDENT LEGAL SERVICES, *supra* note 62; Facebook.com, About Facebook, <http://www.facebook.com/about.php> (last visited Nov. 30, 2007); Facebook.com, Facebook’s Privacy Policy, <http://www.facebook.com/policy.php> (last visited Nov. 30, 2007); MySpace.com, About Us, <http://www.myspace.com/index.cfm?fuseaction=misc.aboutus> (last visited Nov. 30, 2007); MySpace.com, Privacy Policy, <http://www.myspace.com/index.cfm?fuseaction=misc.privacy> (last visited Nov. 30, 2007).

64. See Cyber Safety Glossary, *supra* note 60.

65. TechEncyclopedia from TechWeb Network, Social Networking Site, <http://www.techweb.com/encyclopedia/defineterm.jhtml?term=SOCIALNETWORKINGSITE> (last visited Oct. 27, 2007).

66. See *infra* notes 67-71 and accompanying text.

67. See Brandon Meachum, *Schools Warn: MySpace Is Not Just Your Space*, DENVER POST, Aug. 27, 2006, at B01; see also Brian Deagon, *Though MySpace, Facebook Dominate, Others Seek Social Networking Niches*, INVESTOR’S BUS. DAILY, Sept. 24, 2007, at A06 (discussing the popularity of MySpace and Facebook, as well as opportunities for future growth). See generally Facebook.com, <http://www.facebook.com> (last visited Oct. 27, 2007); MySpace.com, <http://www.myspace.com> (last visited Oct. 27, 2007).

68. *MySpace Attracts Older Audience*, WALL ST. J., Oct. 6, 2006, at B4. A “unique visitor” is a statistic describing a unit of traffic to a Web site within a specified time-frame, and is calculated by

[s]oftware that tracks and counts Web site traffic[,] distinguish[ing] between visitors who only visit the site once and *unique visitors* who return to the site. Different from a site’s hits or page views—which are measured by the number of files that are requested from a site—unique visitors are measured according to their unique IP addresses, which are like online fingerprints, and unique visitors are counted only once no matter how many times they visit the site.

Webopedia, Unique Visitor, [http://www.webopedia.com/TERM/U/unique\\_visitor.html](http://www.webopedia.com/TERM/U/unique_visitor.html) (last visited Oct. 27, 2007). However, it is important to note that measuring web traffic in terms of unique visitors has recently been criticized, as some Internet Service Providers use different IP addresses “for every file requested, making one visitor look like many. In this case, a single IP address does not indicate a unique visitor.” *Id.*

users.<sup>69</sup> Furthermore, it is estimated that 85 percent of students at participating universities have a profile registered on Facebook, and 60 percent of those students log in to their profiles daily.<sup>70</sup> Facebook also claims to be the largest photograph-sharing site in the United States and the sixth-most trafficked site in the United States.<sup>71</sup>

One of the distinguishing features of these social networking sites has been their eligibility requirements. MySpace generally permits anyone to join and create a profile, with minimal restrictions on who can join.<sup>72</sup> In contrast, Facebook originally only permitted individuals with a university email address (.edu address), a high school email address, or members of certain companies and organizations to join.<sup>73</sup> However, Facebook recently decided to open its doors to everyone, allowing individuals to join Facebook networks based on their geographic location, such as their city or state.<sup>74</sup> In the past, employers gained access to the Facebook profiles of applicants by signing up for alumni email addresses with their alma maters—in order to allow them access to Facebook—or by asking college student interns to “perform online background checks” on applicants.<sup>75</sup> Facebook’s new policy may make it easier for employers to access information about applicants on Facebook without taking these additional steps to create accounts.

With so many individuals sharing such a vast amount of information on these social networking sites, it has become increasingly easier for employers to obtain information about applicants that was once unavailable to them.<sup>76</sup> MySpace and

---

69. Facebook.com, Statistics, <http://www.facebook.com/press/info.php?statistics> (last visited Oct. 27, 2007).

70. Posting of Michael Arrington to TechCrunch, 85% of College Students Use FaceBook (Sept. 7, 2005), <http://www.techcrunch.com/2005/09/07/85-of-college-students-use-facebook>.

71. Facebook.com, Statistics, *supra* note 69. However, it is important to take these statistics with a grain of salt. As Nate Elliot, a Jupiter Research analyst, notes, while there is a lot of traffic on these social networking sites, the sites are “promoting the number that is most advantageous for them to promote.” Jonathan Silverstein, *Is MySpace.com Really That Popular? Analyst Questions the Site’s User Numbers and Sustainability of the ‘Cool Factor’*, ABC NEWS, Feb. 22, 2006, <http://abcnews.go.com/technology/story?id=1650209>. While there is admittedly some discrepancy in the number of users for these sites, there is no doubt that both MySpace and Facebook have a staggering number of users and are continuing to increase in popularity.

72. See Finder, *supra* note 3, at 1.

73. Anick Jesdanun, *Facebook Site to Expand Eligibility to All Web*, CINCINNATI POST, Sept. 16, 2006, at A6.

74. See *id.*

75. Finder, *supra* note 3, at 1.

76. See Befort, *supra* note 12, at 370-71.

Facebook, along with other similar social networking sites, "have created huge new portals for the mass disclosure of private information."<sup>77</sup> Employers have taken note of this trend and have begun scouring the Internet to research applicants further.<sup>78</sup> While the privacy policies of these social network sites aim to prevent unwanted disclosure, the availability of information on these sites creates the potential for previously nonexistent legal and ethical issues to arise in employment relationships.<sup>79</sup>

### *B. Applicants Under Investigation*

With the increasing popularity of MySpace and Facebook has come a growing trend among employers to conduct online background checks of job applicants by searching their MySpace and/or Facebook profiles.<sup>80</sup> Michael Sciola, director of the career resource center at Wesleyan University in Middletown, Connecticut, believes such background investigation into social networking sites is "a growing phenomenon" and referred to it as the next step for employers after Googling applicants.<sup>81</sup> Similarly, Microsoft admits that "researching students through social networking sites [is] now fairly typical."<sup>82</sup> Warren Ashton, group marketing manager at Microsoft, indicated "[i]t's becoming very much a common tool."<sup>83</sup>

Searches of applicant profiles have often resulted in unfavorable outcomes for applicants. According to a 2005 study conducted by ExecuNet, an executive job-search agency, "75 percent of recruiters already use Web searching as part of the applicant screening process," and "[m]ore than a quarter of these same recruiters say they have eliminated candidates based on information they found online."<sup>84</sup> Similarly, NBC News reported that "a recent survey shows that over 77 percent of employees uncover information about candidates online, and 35 percent of them have eliminated

77. Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 880 n.16 (2006).

78. See Finder, *supra* note 3, at 1.

79. See *Hiring: Pitfalls*, *supra* note 11, at 5.

80. See Finder, *supra* note 3, at 1; accord Lydia West, *Employers Use Facebook as an Employment Tool*, STUDENT VOICE, Sept. 6, 2006, available at <http://media.www.asustudentvoice.com/media/storage/paper895/news/2006/09/06/CampusLife/Employers.Use.Facebook.As.An.Employment.Tool-2900039.shtml>.

81. Finder, *supra* note 3, at 1.

82. *Id.*

83. *Id.*

84. Jimmy Greenfield & David Haugh, *When What Happens on MySpace Doesn't Stay on MySpace*, CHI. TRIB., Mar. 28, 2006, at C1.

candidates based on information they have uncovered.”<sup>85</sup> A poll by the National Association of Colleges and Employers found that almost 27 percent of 254 surveyed employers admitted to reviewing applicants’ profiles on social networking sites, such as MySpace and Facebook, before hiring them.<sup>86</sup> It is clear that employers are increasingly checking the social networking profiles of their applicants and that those applicants may suffer as a result of the information they have posted on the Internet.

An anecdote reveals the powerful effect such background investigations may have. The president of a small consulting company in Chicago logged onto Facebook to research a recent University of Illinois graduate who was applying for a summer intern position.<sup>87</sup> On the site the president found the applicant’s profile, which listed his interests as “smokin’ blunts” . . . , shooting people and obsessive sex, all described in vivid slang.”<sup>88</sup> Needless to say, in this case the applicant’s Facebook profile prevented him from getting the job.<sup>89</sup> “What once was considered a private realm for the younger generation is becoming widely known to the older generation,” and employers are increasingly capitalizing on the informational abundance provided by this new realm.<sup>90</sup>

In this emerging area of law, the focus has been on the negative impact an applicant’s social networking profile may have on his or her employment opportunities.<sup>91</sup> However, there are also several potential benefits for applicants who have professional social networking profiles. Social networking profiles can serve as a cheap, efficient way for applicants to provide positive, professional information about themselves, and they may also help applicants “build visibility and credibility as an expert” in their field or interests.<sup>92</sup> A survey conducted by CareerBuilder.com found that “hiring managers said 64 percent of candidates’ background information supported their professional qualifications for the job, 40 percent of candidates were well-rounded and showed a wide range of interests and 31 percent of candidates’ sites conveyed a professional

---

85. *NBC Nightly News: Profile: College Students Using New Web Site Could Have Their Personal Information Read by Prospective Employers* (NBC television broadcast May 13, 2006) (transcript available at 2006 WLNR 8296767).

86. *Hiring: Pitfalls*, *supra* note 11, at 4.

87. *See Finder*, *supra* note 3, at 1.

88. *Id.*

89. *See id.*

90. STUDENT LEGAL SERVICES, *supra* note 62.

91. *See supra* notes 84-90 and accompanying text.

92. *Employers Using Facebook Part I*, *supra* note 10.

image.”<sup>93</sup> As employers continue to search applicants’ social networking profiles, they are also beginning passively to recruit individuals based on information found on applicants’ social networking profiles.<sup>94</sup> For example, Catherine Germann, a 2005 Information Technology graduate from the Rochester Institute of Technology,

was in the midst of her job search, [when] she was contacted out of the blue by a recruiter. He had seen Germann’s resume on a job board and promptly Googled her name, finding her personal website, her live journal and noticed that they had a mutual friend. Germann had already cleaned up her personal pages and adjusted the privacy settings to project a more professional image. Her site helped her in a positive way to build a potential job connection.<sup>95</sup>

Therefore, applicants who maintain a positive, professional social networking profile may not only find their potential employers more receptive to their applications, but may also obtain additional employment opportunities from other employers who find them on social networking sites.

### III. POTENTIAL LEGAL ISSUES ARISING FROM EMPLOYER INVESTIGATION OF APPLICANTS’ SOCIAL NETWORKING PROFILES

Up to this point, employers have generally felt that “they are on safe ground looking at profiles on MySpace or Facebook because there are currently no laws stopping them from doing so.”<sup>96</sup> Furthermore, employers believe they have the right to obtain as much information as possible about applicants and that using social networking sites “is fair game to find out who will be the ‘best fit’ for their organization.”<sup>97</sup> Many employment attorneys believe there is nothing illegal about employers using social networking sites to uncover additional information about applicants, but this is not entirely clear.<sup>98</sup>

While searching applicants’ social networking profiles may not be illegal in itself, legal issues may potentially arise if employment decisions are made based on information discovered during these

---

93. Katie Pircher, *MySpace EmployerSpace: As Graduates Attempt to Get Jobs, Employers May Also Be Facebooking and MySpacing to See What Their Potential Employees are Doing Online*, THE DEPAULIA, <http://www.thedepaulia.com/story.asp?artid=1932&sectid=1> (last visited Oct. 26, 2007).

94. Press Release, MySpace Is Public Space When it Comes to Job Search, *supra* note 1.

95. *Id.*

96. *Hiring: Pitfalls*, *supra* note 11, at 5.

97. *Id.* at 4.

98. *See id.* at 5.

searches. As Chris Wolf, a partner at the law firm of Proskauer Rose LLP, has pointed out, no cases exist that address an employer's review of social networking sites as a basis for making employment decisions, thus making this "an emerging area of law."<sup>99</sup> While there have been numerous cases involving employees who sued after being fired for Internet postings (mainly blogs), a case has yet to arise dealing with social networking profiles of applicants seeking employment.<sup>100</sup> With the plethora of legal issues that may arise from employer reviews of applicants' social networking profiles, it seems likely that such a case will arise in the near future.

This new method of employer information gathering is extremely different from its predecessors.<sup>101</sup> Most noticeably, social networking sites have produced a vast increase in the amount of applicant information that is readily available to and easily accessible by employers. Despite this stark difference, basic employment laws still apply to employers seeking information on social networking sites, which raises several potential legal issues.<sup>102</sup> Potential suits that may arise in this context include claims of invasion of privacy, discrimination, violation of terms of service of the sites, violation of the FCRA, and defamation. However, these claims must be analyzed in light of the general rule in the employment setting—the employment at will doctrine,<sup>103</sup> which generally permits employers to base their hiring decisions on good reasons, bad reasons, arbitrary reasons, or no reason at all, so long as they do not violate any specific laws in the process.<sup>104</sup> Therefore, while many applicants may not like the idea of employers making adverse employment decisions based on their social networking profiles, it seems that employers have a significant amount of leeway to do so, as long as they do not violate a specific law.

### *A. Invasion of Privacy*

Invasion of privacy is one of the issues most commonly cited by applicants who feel that employers should not be looking at their

---

99. *Id.*

100. *See id.*

101. *See supra* Part I.

102. *See Ford & Harrison, LLP, What You Won't See on a Resume*, GA. EMP. L. LETTER, July 2006, at 5.

103. *See generally* Wendy Parker, *Lessons in Losing: Race Discrimination in Employment*, 81 NOTRE DAME L. REV. 889, 927-28 (2006) (discussing the judicial commitment to the employment at will doctrine).

104. *Id.* at 927.



social networking profiles when making employment decisions.<sup>105</sup> This is likely due in large part to the applicants' misperception that much of what they do and post on social networking sites is private.<sup>106</sup> There is a significant difference between the amount of privacy applicants believe they have in regards to their social networking activity and the amount of privacy that actually exists on these sites.<sup>107</sup> This misperception is reinforced by the social networking sites themselves, as evidenced by Facebook's "Frequently Asked Questions" section.<sup>108</sup> The Facebook website states that it allows users to restrict the availability of their profiles to ensure that "your information is seen by people you want to share it with, and not by people you don't."<sup>109</sup> However, while it is true that Facebook and other social networking sites have privacy settings that allow users to restrict the availability of their profiles in certain ways,<sup>110</sup> the information is not as private as many users believe. Furthermore, the

105. See, e.g., Cristian Lupsa, *Facebook: A Campus Fad Becomes a Campus Fact; The Social-Networking Website Isn't Growing Like It Once Did, but Only Because Almost Every US Student is Already on It*, CHRISTIAN SCI. MONITOR, Dec. 13, 2006, at 13 (discussing research findings that 42 percent of students and 21 percent of employers thought that an employer's use of Facebook violated privacy rights); West, *supra* note 80 (quoting one college student as arguing that, "[w]ithout prior warning, looking at a candidates' Facebook profile and judging them based on that is unethical. It's crossing our line of privacy").

106. See Posting of Tim Armstrong to Info/Law, Social Darknets, <http://blogs.law.harvard.edu/infolaw/2006/06/12/social-darknets/> (June 12, 2006) (discussing how this "illusion of relative anonymity . . . has been punctured"); see also Digital Garbage, Facebook: Job-Hunting, Non-Invisibility, and the Creepiness Factor (June 12, 2006), <http://digitalgarbage.net/2006/06/12/facebook> ("Although names like 'MySpace' paint an image of personal spaces, personal doesn't mean private.").

107. Posting of Tim Armstrong, *supra* note 106.

108. See Employers Using Facebook Part I, *supra* note 10 (arguing that Facebook supports a reasonable expectation of limited access, but not necessarily of privacy).

109. Facebook Search and Browse Help, <http://www.facebook.com/help.php?page=10> (last visited Oct. 26, 2007).

110. For example, users can adjust their privacy settings to limit other users' ability to view their profiles (i.e., they can allow only their "friends" or people in their networks to view their profiles, or they can allow anyone to view their profiles), to limit what information on their profiles can be seen by users viewing their profiles, and to limit the ability of other users to find their profiles when searching the site. Facebook.com, Facebook's Privacy Policy, <http://www.facebook.com/policy.php> (last visited Nov. 30, 2007); MySpace.com, Privacy Policy, <http://www.myspace.com/index.cfm?fuseaction=misc.privacy> (last visited Nov. 30, 2007). Facebook has "specific privacy settings for photos, notes, each part of your profile and more. You can block individuals you don't want knowing you exist on Facebook, and you can create a Limited Profile to hide certain parts of your profile from specific friends." Facebook.com, Privacy Controls, <http://www.facebook.com/sitetour/privacy.php> (last visited Nov. 30, 2007). Ultimately, users choose what information is included in their profiles, and the privacy settings allow users to control the other users with whom that information is shared. Facebook.com, Facebook's Privacy Policy, <http://www.facebook.com/policy.php> (last visited Nov. 30, 2007).

privacy features on these sites require users to take action to limit their profile to certain viewers. Many users are unaware of this, and “only a small number of members change the default privacy preferences, which are set to maximize the visibility of user profiles.”<sup>111</sup> This creates in users “a sense of false security that they’re broadcasting only to their personal crowd.”<sup>112</sup> Despite applicants’ beliefs that much of what they do on social networking sites is private, it is clear that this is not the case, as employers continue to access this information.<sup>113</sup>

While claims that employers are invading applicants’ privacy by looking at their social networking profiles may be the most common, they are the least likely to succeed. As stated above, to be successful on an invasion of privacy claim the applicant must have had a “reasonable expectation of privacy” regarding the information.<sup>114</sup> While many applicants believe they have a reasonable expectation of privacy regarding their social networking activity, this is a difficult argument to support. This is in large part because courts often consider information available on the Internet to be in the public domain.<sup>115</sup> Since the information on social networking sites is posted on the Internet, “the rule of thumb is: If it’s in the public domain, it’s fair game.”<sup>116</sup> It is difficult to imagine that an applicant would be able to claim successfully a “reasonable” expectation of privacy to information in the public domain.

Further weakening an invasion of privacy claim is the fact that the information on these social networking sites is voluntarily disclosed and posted in the public domain by the applicants themselves. As attorney Jim Erwin, head of the employment group at Pierce Atwood LLP in Portland, Maine, points out, “People who post information on the Internet don’t have a reasonable expectation of

---

111. Ralph Gross et al., *Information Revelation and Privacy in Online Social Networks*, PROC. 2005 ACM WORKSHOP ON PRIVACY ELECTRONIC SOC’Y, 71, 79 (2005).

112. Digital Garbage, *supra* note 106.

113. See *supra* Part II.B (discussing various employers’ uses of social networking sites to investigate applicants).

114. Employers Using Facebook Part I, *supra* note 10; see *California v. Greenwood*, 486 U.S. 35, 41 (1988); *supra* Part I.

115. See Michael Whiteman, *The Impact of the Internet and Other Electronic Sources on an Attorney’s Duty of Competence Under the Rules of Professional Conduct*, 11 ALB. L.J. SCI. & TECH. 89, 97 (2001).

116. Martha Irvine, *When MySpace Becomes Everyone’s Space*, GLOBE & MAIL (Toronto), Dec. 30, 2006, at R12.

privacy, so they shouldn't be shocked that companies are researching them by these means."<sup>117</sup>

This is not to say that an applicant stands no chance of successfully asserting an invasion of privacy claim. If an applicant using a social networking site utilizes the privacy features offered by the site and "an employer somehow hacks past such a privacy barrier, [the applicant] may have a strong privacy claim."<sup>118</sup> However, even if an employer hacks past an applicant's privacy settings, it remains unlikely that an applicant who voluntarily posts information on the Internet will succeed on an invasion of privacy claim because the information is still in the public domain. "[I]t would be tough to claim that this expectation of limited access, even if reasonable, is an expectation of 'privacy.'"<sup>119</sup> To be safe, applicants should assume that anything that is posted in the public domain is not private.<sup>120</sup> Applicants should be aware that "anything they post on-line, even to a site that offers limited password protection such as Facebook, is information that can potentially be accessed by anyone at anytime and forever."<sup>121</sup>

### B. Discrimination

An adverse employment decision based on the social networking profile of an applicant may potentially violate anti-discrimination laws. As detailed above, Title VII and the ADA prohibit discrimination based on an applicant's race, color, religion, sex, or national origin, or based on an applicant's disability, respectively.<sup>122</sup> Quite often, all of this information is available on an applicant's social networking profile, in addition to information about the applicant's sexual orientation, political affiliation, age, and marital status.<sup>123</sup> While the availability of this information does not

---

117. Matt Wickenheiser, *Job Seekers: Beware Your Web Persona; More Companies are Turning to Sites Such as MySpace to Research Prospective Employees*, PORTLAND PRESS HERALD, Aug. 25, 2006, at C1.

118. Employers Using Facebook Part I, *supra* note 10.

119. *Id.*

120. See Diane E. Lewis, *Job Applicants' Online Musings Get Hard Look*, BOSTON GLOBE, Mar. 30, 2006, at A1 (quoting Tal Morse, chief executive of VerifiedPerson, as stating that "the public needs to understand . . . that whenever information is in the general domain, assume it is not private").

121. Posting of Steven Rothberg to CollegeRecruiter.com, NBC Interview, [http://www.collegerecruiter.com/weblog/archives/2006/05/nbc\\_interview.php](http://www.collegerecruiter.com/weblog/archives/2006/05/nbc_interview.php) (May 14, 2006, 19:27 EST).

122. See *supra* text accompanying notes 18-28.

123. George's Employment Blawg, Employers Using Facebook for Background Checking, Part III, <http://www.employmentblawg.com/2006/employers-using-facebook-for->

inherently lead to discrimination, employers who make adverse employment decisions based on an applicant's social networking profile may find themselves subject to discrimination claims. "These topics typically are off limits in job interviews because they can be grounds for discrimination suits if people aren't hired."<sup>124</sup>

Although questions regarding all of these topics are not necessarily illegal, employers generally avoid asking them because they typically have "no legitimate, job-related reason for asking them, and they are suggestive of unlawful discriminatory motives."<sup>125</sup> While social network researching is a new method for investigating applicants, the basic employment laws still apply.<sup>126</sup> Employers cannot base their hiring decisions on information that an applicant is a certain race, age, religion, gender, or national origin, nor can employers base hiring decisions on information that an applicant has a particular disability.<sup>127</sup>

It is clear that some of these factors, such as race, sex, color, and perhaps age, would become evident to an employer during an interview; however, the employer would not likely know those factors during the earlier stages of the application process, when employers are screening the applications and resumes.<sup>128</sup> Information regarding marital status, sexual orientation, and political affiliation would not be known unless volunteered by the applicant or directly asked about by the employer.<sup>129</sup> Therefore, employers that make hiring decisions based on applicants' social networking profiles may find it difficult to defend against a claim that this information was used as the basis for their hiring decisions. This would be particularly true if it was found that applicants with a certain characteristic of a protected class—race, sex, age, or disability—were being systematically refused by employers who viewed applicants' social networking profiles at the earlier stages of the applications process.

For example, suppose an employer with a roughly equal number of similarly qualified Caucasian and African-American applicants checks the social networking profiles of each of the

---

background-checking-part-iii/ (Dec. 10, 2006, 21:32 CST) [hereinafter *Employers Using Facebook Part III*].

124. Ed Frauenheim, *Caution Advised When Using Social Networking Web Sites for Recruiting, Background Checking*, WORKFORCE MGMT. ONLINE, Nov. 2006, <http://www.workforce.com/section/06/feature/24/58/49/245851.html>.

125. *See id.*

126. *See What You Won't See on a Resume*, *supra* note 102.

127. *Employers Using Facebook Part III*, *supra* note 123.

128. *Id.*

129. *See id.*

applicants after receiving the applicants' resumes but before offering an interview, and it turns out that no, or substantially fewer, African-Americans are called in for interviews. The employer in this case may have a very difficult time defending itself against a race discrimination claim under Title VII, even if race had nothing to do with its decisions. It is not difficult to imagine a similar situation occurring later in the hiring process if an employer who checks its applicants' social networking profiles systematically refuses to hire applicants of a certain sexual orientation, since some states and municipalities prohibit discrimination on this basis.<sup>130</sup>

Other types of social networking checks by employers could also constitute unlawful discrimination. For example, if an employer only checks the social networking profiles of certain types of applicants, such as African-Americans or women, it may be considered evidence of unlawful discrimination.<sup>131</sup> Even if an employer checks the social networking profiles of every applicant, there may be evidence of unlawful discrimination if "discriminatory bias affects the employer's evaluation of the information obtained."<sup>132</sup> This could occur if an employer views photographs or text on an African-American's social networking profile more negatively than similar photographs or text on a Caucasian's profile.<sup>133</sup> "An employer may view more negatively photos of an African American male, beer in hand, hanging out at a bar with a hip-hop DJ than photos of a white boy, also with beer in hand, hanging out at a rock 'n roll bar with a bunch of other white boys wearing frat T-shirts."<sup>134</sup> Although some of this evidence may be difficult to prove in certain situations, applicants may have viable discrimination claims against employers who use information gleaned from social networking sites in violation of federal and state anti-discrimination laws.

While Title VII and the ADA, along with various state laws, set out factors upon which employers cannot base their hiring decisions, it appears that employers are permitted to refuse to hire an applicant based on other personal information viewed on his or her social networking profile. According to Jeremy Gruber, legal director of the National Workrights Institute, an employer may legally search social networking sites to find out information about applicants.<sup>135</sup>

---

130. See Employers Using Facebook Part I, *supra* note 10.

131. See *id.*

132. *Id.*

133. See *id.*

134. *Id.*

135. See Jessica Mintz, *Career Journal: The Jungle*, WALL ST. J., Mar. 30, 2005, at B6.

Furthermore, “[e]mployers often use non-job-related information about employees’ private lives in making employment decisions,” and “[t]aking such information into consideration is legal, so long as employers don’t violate workplace-discrimination statutes.”<sup>136</sup> It is clear that an employer is prohibited from violating any specific discrimination laws when using information from an applicant’s social networking profile in making hiring decisions. However, it appears to be perfectly legal for an employer to refuse systematically to hire those applicants with drunken, racy, or provocative photographs on their social networking profiles.

### *C. Fair Credit Reporting Act*

A claim under the Fair Credit Reporting Act may not be the first that comes to mind when discussing employer searches of applicants’ social networking profiles. Despite its name, the FCRA applies to much more than credit checks. The FCRA also “governs employment background checks for the purposes of hiring, promotion, retention, or reassignment.”<sup>137</sup> However, the FCRA and its protections “only apply if an employer uses a third-party screening company to conduct and prepare the background check.”<sup>138</sup> Under the FCRA, if a third party prepares a background check on an applicant, the applicant must be “notified that an investigation may be performed,” the applicant must be “given the opportunity to consent,” and the applicant must be notified “if information in the report is used to make an ‘adverse’ decision.”<sup>139</sup>

Since the FCRA only applies when a third party conducts background checks on applicants, the FCRA and its protections do not apply if the employer conducts the background search itself.<sup>140</sup> Therefore, the FCRA will not come into play in the majority of situations where an employer searches applicants’ social networking profiles. However, if an employer hires a third party to search applicants’ profiles, the employer would be bound by the provisions of

---

136. *Id.* (quoting Jeremy Gruber, Legal Director, National Workrights Institute).

137. Privacy Rights Clearinghouse, Fact Sheet 16(a): Employment Background Checks in California (Nov. 2005), <http://www.privacyrights.org/fs/fs16a-califbck.htm#3> (internal quotation marks omitted).

138. Privacy Rights Clearinghouse, Alert: Your Resume’ May Be Overshadowed By Your Online Persona (July 9, 2006), <http://www.privacyrights.org/ar/OnlinePersona.htm>.

139. Privacy Rights Clearinghouse, Fact Sheet 16(a): Employment Background Checks in California, *supra* note 137; see 15 U.S.C. § 1681b(c) (2000).

140. See Privacy Rights Clearinghouse, Fact Sheet 16(a): Employment Background Checks in California, *supra* note 137.

the FCRA.<sup>141</sup> While the FCRA would not prohibit employers from using the information found in applicant profiles, it would at least require the employer to inform applicants that such an investigation would occur and that information from the investigation resulted in the adverse employment decision.<sup>142</sup>

#### *D. Violation of Terms of Service*

Many students and critics have also claimed that employers' use of social networking sites to investigate applicants violates the terms of service of social networking sites.<sup>143</sup> Facebook's terms of service state in part: "You understand that . . . the Service and the Site are available for your *personal, non-commercial* use only."<sup>144</sup> Similarly, the MySpace terms of service state in part: "The MySpace Services are for the *personal use* of Members only and *may not be used in connection with any commercial endeavors* except those that are specifically endorsed or approved by MySpace.com."<sup>145</sup>

Some critics claim that checking an applicant's profile on Facebook or MySpace for purposes of making employment decisions is a commercial use, in direct violation of their terms of service.<sup>146</sup> However, that is far from clear. According to Facebook spokeswoman Brandee Barker, employers conducting background checks of applicants on the site do *not* violate the terms of service of the site if the person conducting the background check is a registered Facebook user and is viewing an applicant's profile as permitted by the privacy settings set by the applicant.<sup>147</sup> Barker stated Facebook's position quite clearly: "It is not a violation of terms of use if one Facebook user views the profile of or communicates with another Facebook user."<sup>148</sup> Declining to comment, MySpace has not yet taken a stance on the

141. See *Employers Using Facebook Part I*, *supra* note 10.

142. See *id.*; see also 15 U.S.C. § 1681b(c) (detailing the requirements placed on employers using third party agencies).

143. See *Frauenheim*, *supra* note 124; see also *Employers Using Facebook Part I*, *supra* note 10 (discussing whether an employer's use of Facebook violates the site's Terms of Use).

144. Facebook.com, Terms of Use, <http://www.facebook.com/terms.php> (last visited Oct. 26, 2007) (emphasis added).

145. MySpace.com Terms of Use Agreement, <http://www.myspace.com/Modules/Common/Pages/TermsConditions.aspx> (last visited Oct. 26, 2007) (emphasis added).

146. *But cf.* *Employers Using Facebook Part I*, *supra* note 10 (recognizing that classifying employer's Facebook use as commercial is "a possible interpretation," but arguing for other interpretations).

147. See *Frauenheim*, *supra* note 124.

148. *Id.*

issue, but its terms provide “another policy,” suggesting that “a recruiter could run afoul of the site’s rules if they gather data on a candidate and share it with others in a company.”<sup>149</sup>

Whether a court would consider an employer’s search of an applicant’s social networking profile to be a commercial use or not is anyone’s guess. However, based on Barker’s statements and other sections of the terms of use, employer investigation of applicants is not the commercial use contemplated by these sites. For example, following Facebook’s stipulation that the site is intended for non-commercial use is a sentence focusing on the materials a user submits to the site through his or her account.<sup>150</sup> Similarly, following MySpace’s non-commercial term is a sentence focusing on commercial advertisements.<sup>151</sup> Therefore, it is quite plausible that the sites’ terms of service prohibiting commercial use of the sites are referring to “posting information for commercial gain, such as advertisements,” rather than the use of the sites to investigate applicants in support of an eventual commercial purpose.<sup>152</sup>

Furthermore, the terms of service for both Facebook and MySpace specifically prohibit using certain types of automated scripts and spamming to collect information from their websites, but do not specifically mention the use of the sites to investigate specific individuals for the purpose of making employment decisions.<sup>153</sup> A clearer violation of the terms of service of these sites may occur if an employer fraudulently gained access to one of the sites by “misrepresent[ing its] affiliation with a college in order to create an account” or by using another’s account to investigate applicants, since these tactics are clearly prohibited by the terms of service.<sup>154</sup> However, such actions may be difficult for an applicant to prove.

---

149. *Id.*

150. See Facebook.com, Terms of Use, <http://www.facebook.com/terms.php> (last visited Oct. 26, 2007). The Terms stipulate that users “represent, warrant and agree that no materials of any kind submitted through [his or her] account . . . will violate or infringe upon the rights of any third party, including copyright, trademark, privacy or . . . libelous, defamatory or otherwise unlawful material.” *Id.*

151. See MySpace.com Terms of Use Agreement, <http://www.myspace.com/Modules/Common/Pages/TermsConditions.aspx> (last visited Oct. 26, 2007). The Terms next address “Proprietary Rights in Content on MySpace.com” and provide, for example, that a user “represent[s] and warrant[s] that . . . the posting of [his] Content on or through the MySpace Services does not violate the privacy rights, publicity rights, copyright, contract rights or any other rights of any person.” *Id.*

152. Employers Using Facebook Part I, *supra* note 10.

153. See *id.*

154. *Id.*



It is important to note that if an employer is found to have violated the terms of service, a federal cause of action may exist under the Federal Computer Fraud and Abuse Act (CFAA)<sup>155</sup> “to the extent that the recruiter/employer exceeded authorized access (as authorized in the terms of service) in obtaining data from a computer system (the [social networking site’s] server).”<sup>156</sup> The CFAA prohibits accessing a computer without authorization.<sup>157</sup> The Terms of Service of many social networking sites prohibit users from accessing their sites by impersonating another person or otherwise misrepresenting themselves.<sup>158</sup> Therefore, under the CFAA, an employer who accesses a social networking site’s server without authorization under the terms of service (as with the employer who gains access to the site’s server through misrepresentation or impersonation) may be subject to both criminal and civil liability.<sup>159</sup>

### *E. Defamation*

A final claim that may arise out of an employer’s investigation of applicants’ social networking profiles is one for defamation brought by an applicant. Jim Erwin provided the following example, explaining how such a defamation claim may arise:

A company does an Internet search on candidate “John Doe” and finds information that Doe did something criminal or morally reprehensible. The company doesn’t check to make sure it’s the same John Doe as the guy being considered for a job and doesn’t do any further investigation. Then the company HR professionals tell other people in the firm that the candidate is linked to that information. If the candidate isn’t the same John Doe and Doe finds out what was said about him, he could sue for defamation.<sup>160</sup>

A defamation claim may be difficult to prove if the employer does not offer the applicant a job and does not tell the applicant what was said about him or her within the company, as the “John Doe” would likely not find out what was said about him otherwise. However, the potential for a defamation claim does exist, and it highlights the need for employers who search applicants’ social networking profiles to be careful with the information they find. As Erwin points out,

---

155. 18 U.S.C. § 1030 (2000 & Supp. 2002).

156. Employers Using Facebook Part I, *supra* note 10.

157. See 18 U.S.C. § 1030.

158. See, e.g., Facebook.com, Terms of Use, <http://www.facebook.com/terms.php> (last visited Oct. 26, 2007) (stating that users “agree not to use the Service or Site to: . . . impersonate any person or entity, or falsely state or otherwise misrepresent yourself, your age or your affiliation with any person or entity”).

159. See 18 U.S.C. § 1030.

160. Wickenheiser, *supra* note 117.

defamation in this context is “not new law or a sticky situation created by technology,” but “the Internet makes it possible to make those mistakes in new ways.”<sup>161</sup>

#### IV. POTENTIAL PITFALLS OF EMPLOYERS’ INVESTIGATION OF APPLICANTS’ SOCIAL NETWORKING PROFILES

While social networking sites can provide employers with a plethora of information about applicants that they would likely not have been privy to otherwise, the sites also have some potential pitfalls of which employers should be aware. The two main problems employers should be concerned with are (1) too much information and (2) issues concerning identity and authenticity.

##### *A. Problem of Too Much Information*

While many employers believe that the more information they can obtain about an applicant the better, “there is such a thing as ‘too much information.’”<sup>162</sup> With so much information readily available and easily accessible on social networking sites, many employers may be tempted to ignore this risk in their endeavor to gain as much information as possible.<sup>163</sup> The reason that too much information can be harmful is because there are some things that employers are better off not knowing. This is particularly true when it comes to defending discrimination claims.<sup>164</sup> As stated above, if employers gain information about applicants from their social networking profiles regarding protected class characteristics—race, sex, color, etcetera—that they would not have otherwise had, they may open themselves up to a slew of discrimination claims from applicants who did not get hired.<sup>165</sup> Once employers have looked at applicants’ social networking profiles, they could not claim that they did not have access to this information, assuming it is listed on the applicants’ profiles. “The flipside is that ignorance of facts related to legally protected characteristics . . . may be a powerful defense to a discrimination charge. (One can’t have based a decision on an unknown fact).”<sup>166</sup> Once an employer looks at an applicant’s social networking profile, the

---

161. *Id.*

162. Employers Using Facebook Part III, *supra* note 123.

163. *Id.*

164. *See id.*

165. *See supra* Part III.B.

166. Employers Using Facebook Part III, *supra* note 123.

defense of ignorance is unavailable. Thus, too much information may bring with it more bad than good.

Similarly, employers attempting to avoid discrimination claims and other types of liability generally tend to request only information from applicants that is job-related because obtaining personal information about an applicant that is irrelevant to his or her ability to perform the job is often seen as a waste of time.<sup>167</sup> Jen Jorgensen, spokeswoman for the Society for Human Resource Management, made this clear: "Just because the information's out there doesn't mean it's useful."<sup>168</sup> In order to avoid the too much information problem, employers obtaining information about applicants "should be carefully constrained to that which is relevant to the job requirements, with potentially sensitive information scrupulously avoided."<sup>169</sup>

### *B. Issues Concerning Identity and Authenticity*

Another serious problem with employers using social networking profiles as tools to investigate applicants is that the profiles they find are not always trustworthy or authentic. While this may seem like an obvious point to many, employers may overlook this concern due to their excitement about this new employment screening tool.<sup>170</sup> As an initial matter, employers should ensure that the information they find on a social networking site is actually about the applicant they are researching and not someone else with the same name.<sup>171</sup> Several Facebook or MySpace profiles may be created by different users with the same name,<sup>172</sup> so if an employer is set on using this employment screening tool, at the very least it should verify the identity of the applicant and ensure that the social networking profile belongs to the applicant in question.

A more important issue regarding employers' use of social networking profiles as an employment screening tool is whether the employers can even trust the information they find on a given site.<sup>173</sup> A recent trend among high school and college students suggests that

167. H.J. Cummins, *Bosses Peek in on Web Site for Students*, SEATTLE POST-INTELLIGENCER, Apr. 3, 2006, at D1.

168. *Id.*

169. Employers Using Facebook Part III, *supra* note 123.

170. George's Employment Blawg, *More on Using Facebook et al. in Recruiting and Hiring* (Part II), <http://www.employmentblawg.com/2006/more-on-using-facebook-et-al-in-recruiting-and-hiring> (Nov. 3, 2006, 1:05 CST) [hereinafter *More on Using Facebook*].

171. Wickenheiser, *supra* note 117.

172. *See generally* Facebook.com, <http://www.facebook.com> (for example, a search of the name "John Smith" on Facebook.com brings up over 500 results).

173. *See More On Using Facebook*, *supra* note 170.

the social networking profile an employer discovers may not be authentic, even if it is the profile of the applicant being investigated.<sup>174</sup> College students have begun creating fake “explicit or unflattering (to say it nicely)” social networking profiles of “people they view as competition for jobs.”<sup>175</sup> Presumably, students believe that if employers look at applicants’ social networking profiles, they will be more likely to hire students who have more appropriate profiles than those who have more explicit ones.<sup>176</sup> The student who is the victim of this hi-tech sabotage may not even know that the fake profile exists, yet he or she may suffer the adverse employment consequences nonetheless.<sup>177</sup> In sum, employers must remember that they cannot necessarily believe everything they find on social networking sites.

As pointed out, the real trouble with employers using social networking profiles as background checks is that the information in these profiles may not be accurate or authentic, and the applicant may never become aware of this fact. This is especially problematic with social networking sites because, “unlike legitimate background check companies, Web sites do not have a duty to investigate potential errors and correct misinformation” about the people who have profiles on their site.<sup>178</sup> Therefore, it is very difficult for an employer to be sure that an applicant’s profile is authentic.<sup>179</sup> “Using such information against the applicant without giving the job seeker a chance to explain or correct the information is unfair, to say the least.”<sup>180</sup> Not only would such a practice be unfair, it would also likely be illegal.<sup>181</sup> This is not to say that employers should never use social networking profiles when investigating applicants. Rather, employers should be aware of the potential pitfalls in doing so, and proceed accordingly.

---

174. Gen Y’d, Recruit on MySpace.com? Better Be Careful!, [http://www.ere.net/blogs/gen\\_yd/C0CA0C1F9171B83E64E8FB7FB466DC84.asp](http://www.ere.net/blogs/gen_yd/C0CA0C1F9171B83E64E8FB7FB466DC84.asp) (Sept. 21, 2006, 15:04 PST).

175. *Id.*

176. *See id.*

177. *Id.*

178. Privacy Rights Clearinghouse, Alert: Your Resume’ May Be Overshadowed By Your Online Persona, *supra* note 138.

179. *Id.*

180. *Id.*

181. *See supra* Part III.

## V. SOLUTION AND RECOMMENDATIONS FOR THE FUTURE

There is no easy solution to the problem caused by employers researching applicants on social networking sites. Applicants want the freedom to express themselves on these sites without having to fear that employers may find this information and refuse to hire them as a result.<sup>182</sup> Conversely, employers want to learn as much as they can about applicants to ensure that they hire the applicant who will be the best fit for their organization, and social networking sites allow them to do this like never before.<sup>183</sup>

One way to solve this problem would be to follow either desire to its extreme. For instance, to give applicants the freedom they desire, employers could be completely banned from looking at social networking sites when making hiring decisions. However, this solution does not seem practical or advantageous. As an initial matter, it would be quite difficult to enforce such a rule. Employers probably would not admit to looking at applicants' social networking profiles in making hiring decisions if there were a rule against doing so, and finding evidence of such behavior may be difficult and time-consuming, as it would require combing through all of the employer's Internet records. However, "the combination of Internet recordkeeping requirements with electronic discovery in litigation" could make finding a violation of this rule easier.<sup>184</sup> It is also unclear what punishment would be appropriate for an employer who violated the rule. Perhaps the most appropriate form of punishment would be monetary compensation for the applicant who was not hired, but it is not clear that a court would agree since no case has been filed on this basis.<sup>185</sup> Furthermore, there are many positive results for both applicants and employers as a result of employers using social networking sites as information-gathering tools.<sup>186</sup>

At the other extreme, to ensure that employers find the best applicant, employers could be given free reign to search social network sites. However, this could effectively force applicants to erase their social networking profiles completely, or at least extremely limit applicants' freedom of expression. Freedom of expression has always been an important value in our society, and online expression, such as occurs on social networking sites, is a healthy and valuable way of

---

182. See *supra* notes 54-57 and accompanying text.

183. See *supra* notes 80-97 and accompanying text.

184. Employers Using Facebook Part III, *supra* note 123.

185. See *supra* notes 99-100 and accompanying text.

186. See *supra* notes 91-95 and accompanying text.

exercising that freedom.<sup>187</sup> Furthermore, giving employers such wide latitude for online searches has other potential pitfalls, such as the problem of too much information and issues concerning identity and authenticity, as discussed above.<sup>188</sup> Therefore, neither of these extreme measures presents a viable solution.

Solving this problem will instead require a compromise between applicants and employers in which both groups recognize the other's concerns. Until a case is decided or a law is passed on the subject, this solution will require voluntary compromise on the part of both applicants and employers. The suggestions that follow offer ways in which such a compromise might be reached.

### *A. Suggestions for Applicants*

To date, there has not been a lawsuit filed against an employer for using social networking sites in conjunction with its hiring decisions, and the legal boundaries of this new employee screening tool are less than clear. Until a definitive judicial decision or legislative decree is announced that addresses these issues, it is safe for applicants to assume that at least some employers will be checking their social networking profiles. Therefore, applicants should operate under the assumption that potential employers will see everything they post on their profiles. With this in mind, it is important for applicants to use discretion in deciding what information to post on their social networking profiles and what information to leave out. If applicants insist on putting certain information on their social networking profiles, they should, at the very least, adjust the privacy settings to restrict access to their profiles.<sup>189</sup>

However, this is not to say that applicants need to erase completely their social networking profiles or that they cannot be themselves on their profiles. Rather, applicants need to be aware that what they post on their social networking profiles may very well be seen by potential employers, and post accordingly. Material that applicants believe to be appropriate for their friends may be considered highly inappropriate by employers: jokes among friends, such as with the University of Illinois graduate who posted “‘smokin’ blunts’ . . . , shooting people and obsessive sex” in his interests section, may have serious ramifications when it comes to the job hunt.<sup>190</sup>

---

187. See *supra* notes 54-65 and accompanying text.

188. See *supra* notes 162-81 and accompanying text.

189. See *supra* notes 110-13 and accompanying text.

190. Finder, *supra* note 3, at 1.

Therefore, instead of posting risqué or drunken photographs from an all-night fraternity party, applicants should recognize the possible ramifications of their actions and keep such material off-line. If someone other than the applicant posts photographs of or information about the applicant on a social networking site or other online site, the applicant should ask the other person to remove the content or ask the site administrator to remove the material.<sup>191</sup>

Many commentators have suggested, and some students have begun following, the so-called “grandmother rule.”<sup>192</sup> The point of this rule is that applicants should not post anything on their social networking profiles that they would not be comfortable showing to their grandmothers.<sup>193</sup> While this may seem a bit extreme to some applicants, others are heeding this advice and benefiting from their social networking profiles.<sup>194</sup> Prudent applicants may also consider searching their names on social networking sites and search engines (like Google) to see what information appears. Doing so will allow applicants to prevent fraudulent accounts with their name from harming their employment chances, and may give applicants an opportunity to warn potential employers that a social networking profile of someone with the same name is not the applicant’s profile.

### *B. Suggestions for Employers*

Employers have an obvious desire to learn as much information as they can about applicants they are considering hiring.<sup>195</sup> However, in addition to the potential pitfalls mentioned above, there are other reasons that employers may want to give applicants some leeway when it comes to social networking profiles. First, employers “should always balance the employer’s need for the information against that of the [applicant’s] privacy.”<sup>196</sup> While employers may like the idea of more fully investigating their applicants, they need to consider how relevant any of the information is to a particular applicant’s job

---

191. See Posting of Nick Douglas to ValleyWag, *How to Look Good When Your Recruiter Googles You*, <http://valleywag.com/tech/silicon-valley-users-guide/how-to-look-good-when-your-recruiter-googles-you-247854.php> (Mar. 28, 2007, 06:11:00 EST); Posting of Austin Groothuis to CALI’s Pre-Law Blog, *Online Content About You Can Hurt You During Your Job Search*, [http://calis\\_pre-law\\_blog.classcaster.org/blog/archives/2007/03/](http://calis_pre-law_blog.classcaster.org/blog/archives/2007/03/) (Mar. 7, 2007).

192. See Posting of Steven Rothberg, *supra* note 121.

193. *Id.*

194. See Press Release, MySpace is Public Space When It Comes to Job Search, *supra* note 1; *supra* notes 91-95.

195. See *supra* notes 12-15 and accompanying text.

196. Ecker, *supra* note 16, at 278.

performance. In all likelihood, most of the negative information on an applicant's social networking profile is irrelevant to job performance, and if the applicant believes this information to be private, it may be more beneficial to the employer to respect this expectation of privacy, whether or not it is reasonable.

Steven Rothberg, president of CollegeRecruiter.com, warns employers that using social networking sites as part of their background checking process could result in a "serious backlash" from college students.<sup>197</sup> Rothberg explains:

Employers which are found out to be using [social networking sites] will likely find that they instantly change from being an employer of choice amongst college students to an employer of last resort. . . . Students infer that their postings to [social networking sites] are private and won't be accessible to employers or other such commercial interests. They'll feel violated and outraged should they find out that an employer has been using [social networking sites] as part of a background checking process.<sup>198</sup>

While the result may not be quite as extreme as to cause students to view such employers as employers of "last resort," Rothberg highlights the potential effect this practice could have on applicants' perception of these employers. Furthermore, employers that use social networking profiles as the basis for employment decisions should ensure that they do so consistently across all legally-protected classes, and should document their searches in the event that disputes arise in the future.<sup>199</sup>

Employers should also keep in mind that just because an applicant does not have a social networking profile does not mean that the applicant is somehow more virtuous than those applicants having a profile.<sup>200</sup> The absence of an applicant's social networking profile does not mean that the applicant's actual background is completely wholesome.<sup>201</sup> An employer may infer that the absence of an applicant's social networking profile shows "probity, circumspection, good judgment, and discretion," but it could just as well be evidence of "technological unsophistication, ignorance, estrangement from the community of one's peers, or an unhealthy self-absorption with one's own public persona."<sup>202</sup> Therefore, employers should keep in mind that the absence of an applicant's social networking profile is not

---

197. Frauenheim, *supra* note 124.

198. *Id.*

199. *See* Employers Using Facebook Part I, *supra* note 10.

200. *See* Posting of Tim Armstrong, *supra* note 106.

201. *Id.*

202. *Id.*



always a good thing, and should factor this in when evaluating candidates who have social networking profiles.

Like applicants, employers may also use social networking sites to their advantage. For example, such sites can help employers find qualified candidates. One way in which employers may do this is to search social networking sites for candidates based on certain educational qualifications or common interests that the employer believes would make an individual a good fit for the company. A more effective way for employers to use social networking sites to their advantage may be to post information about their companies on the sites, describing their company and encouraging individuals to apply. Some companies, such as Microsoft and Osram Sylvania, have begun using social networking sites in this way, "participating openly in online communities to get out their company's messages and to identify talented job candidates."<sup>203</sup> This positive use of social networking sites is a trend that other employers may eventually need to adapt to stay competitive.

Finally, employers researching applicants on social networking sites should keep in mind that they were once young as well. Where youthful indiscretions were once easily forgotten with the passage of time, today's youth and their indiscretions "can be preserved in perpetuity" for all to see.<sup>204</sup> Although applicants should not necessarily feel free to post anything they desire on their social networking profiles with impunity, employers should remember that an applicant's online persona does not always provide an accurate, reliable, or complete picture of the person.

## VI. CONCLUSION

As social networking sites like Facebook and MySpace continue to grow in popularity, employers are catching on to the sites and are using them increasingly for applicant background checks. Through these social networking sites, employers now have access to a plethora of information about applicants that has traditionally been unavailable or off-limits during the hiring process.<sup>205</sup> However, the use of such sites and the information found on them in making hiring decisions presents a variety of legal issues that previously did not

---

203. Finder, *supra* note 3, at 1.

204. Privacy Rights Clearinghouse, Alert: Your Resume' May Be Overshadowed By Your Online Persona, *supra* note 138.

205. See *supra* notes 76-79 and accompanying text.

exist in the hiring process.<sup>206</sup> Consequently, the legal boundaries surrounding the use of such sites in the hiring process are unclear.

While many applicants believe that employers invade their privacy by examining their social networking profiles, privacy claims are unlikely to succeed.<sup>207</sup> Applicants who voluntarily disclose information in the public domain face an uphill battle in attempting to claim privacy to such information, even if the site they are using is password protected.<sup>208</sup> However, other legal issues, such as claims of discrimination, violation of the FCRA, violation of terms of service, and defamation, may succeed if the applicant can prove them with some degree of certainty.<sup>209</sup>

Until a judicial or legislative decision is made regarding employers' use of social networking sites in the hiring process, it is safe for applicants to assume that employers will, in fact, search their social networking profiles when making hiring decisions. As such, applicants should take appropriate steps to protect themselves. For some, this may mean sanitizing their profiles. For others, this may simply entail utilizing the privacy features offered by these sites to restrict access to their profiles. Regardless of what steps are taken, applicants must recognize that, at this point, virtually anything they say, do, or post online may be used for or against them during their employment search. While employers keep clicking away, applicants should protect themselves accordingly.

*Ian Byrnside\**

---

206. See *supra* notes 79-100 and accompanying text.

207. See *supra* Part III.A.

208. See *supra* notes 118-21 and accompanying text.

209. See *supra* notes 122-61 and accompanying text.

\* J.D. Candidate, Vanderbilt University Law School, 2008; B.A., Psychology, Duke University, 2005. The author wishes to thank the following people: his parents and his girlfriend, Donya Mir, for their endless love, support, and encouragement; and the editorial staff of the *Vanderbilt Journal of Entertainment and Technology Law* for their hard work and assistance.

