2012

It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act

Nathan J. Ebnet

Note

It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act

Nathan J. Ebnet∗

Landing that great new job just got a little bit harder. In addition to written applications, lengthy interviews, and comprehensive criminal and credit checks, a growing number of employers are factoring job candidates' social media profiles into their hiring decisions.[1] Even in 2006, roughly thirty-five percent of employers eliminated job candidates based on information discovered online.[2] And although it should come as no surprise that more obscene social media content, such as sexually explicit photos or racist remarks, could damage an individual's job prospects, so too could a long-forgotten blog post or a heated political discussion with a friend.[3] After all, only a few clicks separate a staggering amount of personal data—conveniently preserved online—from a curious employer.[4]

Despite the increasing popularity of social media pre-employment screening, whether or not such a practice is legal

∗ J.D. Candidate 2013, University of Minnesota Law School; B.A. 2009, Gustavus Adolphus College. The author would like to give special thanks to Professor Stephen Befort for his invaluable assistance throughout the writing process. Many thanks also to the hardworking editors and staff members of the *Minnesota Law Review*. Above all, the author expresses gratitude to his family and friends.

1. *See* Jennifer Preston, *Social Media History Becomes a New Job Hurdle*, N.Y. TIMES, July 21, 2011, at B1.

2. *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).

3. *See* Ian Byrnside, Note, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 446 (2008) (contrasting information regarding a user's favorite band or movie to posts that feature a person's sexual escapades and substance abuse).

4. *See id.* at 455–56.

or appropriate is a subject of disagreement.[5] Many employers applaud social media pre-employment screening because it allows them to gather as much information as possible about job applicants, making it easier to predict the likely match between the applicant and the job.[6] On the other hand, some commentators argue that employers should be wary of using social media to evaluate job candidates.[7] Citing concerns over the trustworthiness and authenticity of information obtained from the Internet,[8] along with the potential for its abuse,[9] privacy experts encourage employers to look elsewhere for applicant data.[10]

Sharp disagreement over the legality of social media pre-employment screening persists because the accessibility of social media challenges the regulatory framework governing traditional pre-employment screening practices.[11] For example, the Fair Credit Reporting Act (FCRA), which contains notice and consent requirements for a wide variety of background checks that are particularly relevant to the social media pre-employment screening context, only applies to those background checks conducted by third-party screening companies.[12] Since most employers obtain and view an applicant's social me-

5. *See id.* at 458 ("Many employment attorneys believe there is nothing illegal about employers using social networking sites to uncover additional information about applicants.").

6. *See id.* ("[E]mployers 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.'" (quoting *Hiring: Pitfalls of Checking Job Applicants' Personal Web Pages*, MANAGING ACCOUNTS PAYABLE, Oct. 2006, at 5)).

7. *See, e.g.*, Rachel Slagle, *Approach Social Media Sites with Caution in the Pre-Employment Screening Process*, INSPERITY (Oct. 5, 2011), http://www.insperity.com/blog/article/approach-social-media-sites-with-caution-in-the-pre-employment-screening-proces/.

8. *See* Byrnside, *supra* note 3, at 476 ("[E]mployers should remember that an applicant's online persona does not always provide an accurate, reliable, or complete picture of the person.").

9. For a discussion of discrimination in the hiring process, see Stephen F. Befort, *Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place*, 14 HOFSTRA LAB. & EMP. L.J. 365, 381 (1997).

10. *See* Carolyn Elefant, *Do Employers Using Facebook for Background Checks Face Legal Risks?*, LAW.COM LEGAL BLOG WATCH (Mar. 11, 2008, 3:45 PM), http://legalblogwatch.typepad.com/legal_blog_watch/2008/03/do-employers-us.html ("I think it's unlikely employers are going to learn a good deal of job-related information from a Facebook page they won't learn in the context of a well-run interview, so the potential benefit of doing this sort of search is outweighed by the potential risk.").

11. *See* Byrnside, *supra* note 3, at 458–59.

12. Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681t (2006).

dia information from a work or personal computer without the assistance of a third-party screening company, this type of informal research escapes the restrictions of the FCRA and many other regulations designed to protect an applicant's privacy.[13]

However, just like so many other aspects of the Internet, social media pre-employment screening is evolving.[14] With acquiescence from the federal government,[15] several start-up companies now offer to research job candidates' online activities for employers. Boasting of a superior method of social media research, these start-up companies hope to persuade employers to abandon "in-house" social media screening in favor of a formal third-party report.[16] Consider Social Intelligence, a company founded in 2010 in Santa Barbara, California.[17] It scours the Internet for everything job applicants may have said or done online in the past seven years and then provides employers a specialized social media report detailing an applicant's online activity.[18] When social media pre-employment screening is performed by third parties like Social Intelligence, it must be FCRA compliant.[19] Yet employers remain free to avoid the restrictions of the FCRA by simply conducting in-house online research rather than contracting with third parties.[20] This problematic loophole highlights the need for further analysis in this emerging area of the law.

This Note argues that FCRA compliant third-party social media screening appropriately balances the privacy interests of job applicants with the information appetite of employers. Part I describes traditional applicant screening strategies, how they are regulated, and the distinctive privacy interests threatened by employers' informal use of social media during the hiring process. Part II analyzes the utility and application of existing regulatory methods to social media background checks. Finally,

13. *See* Byrnside, *supra* note 3, at 459 (noting that social media has increased the amount of applicant information "that is readily available to and easily accessible by employers").

14. *See* Preston, *supra* note 1, at B1.

15. *See* Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., Bureau of Consumer Prot., Fed. Trade Comm'n, to Renee Jackson, Esq., Nixon Peabody LLP (May 9, 2011), *available at* www.ftc.gov/os/closings/110509social-intelligenceletter.pdf.

16. *See* Preston, *supra* note 1, at B1.

17. *Id.*

18. *Id.*

19. *See* Mithal, *supra* note 15, at 2.

20. *See* Byrnside, *supra* note 3, at 465.

Part III contends that the FCRA is uniquely suited to address the legal problems arising from social media use in the hiring arena. Therefore, this Note recommends that all social media screening should be formalized—by requiring employers to hire third-party companies to perform social media research and submit to the FCRA, employers will obtain reliable applicant information and respect candidate privacy.

I. EMPLOYERS' PRE-EMPLOYMENT SCREENING PRACTICES: THEN AND NOW

In today's hyper-competitive market,[21] employers likely have the luxury of choosing from many highly qualified applicants for any particular job opening.[22] Still, employers routinely "screen in" applicants who possess desirable characteristics and "screen out" applicants with negative traits.[23] Ultimately, they try to find applicants with qualities that will maximize work productivity and minimize costs and liability.[24]

To aid in this search, employers use an assortment of familiar pre-employment screening practices, including interviews and background checks.[25] But due to the likelihood that even seemingly benign screening activities will go too far, traditional pre-employment screening is subject to a variety of legal restrictions that attempt to protect applicants from an overly intrusive hiring experience.[26] New technologies threaten this regulatory landscape.[27] Specifically, the advent of social media offers employers convenient access to previously unobtainable

21. The national jobless rate for the United States during January 2012 was 8.3 percent. *See* Press Release, U.S. Dep't of Labor, The Employment Situation—January 2012 (Feb. 3, 2012), *available at* http://www.bls.gov/news.release/archives/empsit_02032012.pdf.

22. *See* Catherine Rampell, *Many with New College Degree Find the Job Market Humbling*, N.Y. TIMES, May 19, 2011, at A1 (stating that about only half of the jobs landed by new college graduates require a college degree).

23. *See* Ann Marie Ryan & Marja Lasek, *Negligent Hiring and Defamation: Areas of Liability Related to Pre-Employment Inquiries*, 44 PERSONNEL PSYCHOL. 293, 304 (1991).

24. Byrnside, *supra* note 3, at 448; *see also* JOSEPH ZEIDNER & CECIL D. JOHNSON, THE ECONOMIC BENEFITS OF PREDICTING JOB PERFORMANCE, VOL. I: SELECTION UTILITY 143 (1991) (positing that pre-employment "[t]esting can save [employers] money because employees selected by valid tests are more productive than those selected by other methods").

25. *See* Byrnside, *supra* note 3, at 448.

26. *See id.* at 379–80.

27. *See id.* at 370–71 (suggesting that technological advances are likely to continue to provide employers with new and sophisticated screening technology).

applicant information.[28] Employers are implementing this powerful new hiring tool, justifying an examination of social media pre-employment screening.

A. THE LEGAL CONSTRAINTS ON TRADITIONAL PRE-EMPLOYMENT SCREENING

Historically, employers relied on written applications, questionnaires, interviews, references and background checks to screen job applicants.[29] These practices were presumed permissible, limited only by certain exceptions designed to preserve the privacy of job candidates.[30] If an employer appropriately balanced the prospective employee's right to privacy with the employer's own right to hire a qualified individual, the pre-employment screen was reasonable.[31] However, within recent years, even traditional pre-employment screening practices have received heightened judicial and legislative scrutiny.[32] In particular, traditional pre-employment research is subject to the anti-discrimination constraints of Title VII of the Civil Rights Act of 1964 (Title VII) and the Americans with Disabilities Act (ADA), state statutes regarding arrest records, the reporting restrictions of the FCRA, and the privacy protections contained in the Fourth Amendment.[33]

1. Title VII and the ADA

Title VII, the main federal anti-discrimination statute, forbids employers from discriminating against applicants based on race, color, religion, sex, or national origin.[34] Critically, Title VII does not prohibit application procedures that elicit information concerning a protected class as long as employment decisions are grounded in legitimate, non-discriminatory mo-

28. *See* Byrnside, *supra* note 3, at 446–47 ("[P]rospective employers are becoming increasingly aware of [social networking] sites and are taking advantage of the massive amount of newly available information to assist them in them in their hiring decisions.").

29. *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, 255–61 (1994) (describing traditional methods of pre-employment screening).

30. LEX K. LARSON, EMPLOYMENT SCREENING § 9.01 (1992).

31. Ecker, *supra* note 29, at 254–55.

32. *See* Befort, *supra* note 9, at 366.

33. *See id.* at 381.

34. *See* Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e–2000e-17 (2006).

tives.[35] Guidelines promulgated by the Equal Employment Opportunity Commission (EEOC) state that interview questions that either directly or indirectly require the disclosure of information concerning protected class status may constitute evidence of discrimination.[36]

Similarly, the ADA prohibits discriminatory hiring against individuals with a disability who, with or without reasonable accommodation, can perform the essential functions of the employment position.[37] But the ADA goes a step further than Title VII: it actually prohibits employers from inquiring about the existence, nature, or severity of a disability even if the responses are not used in making an employment decision.[38] As a general rule, employers may investigate an applicant's abilities but may not seek information concerning impairment status.[39]

It is important to note that state statutes frequently supplement Title VII and the ADA.[40] In Minnesota, for example, state law prohibits pre-employment inquiries concerning race, religion, color, national origin, ancestry, sex, age, creed, marital status, disability, status with regard to public assistance, and sexual orientation.[41] And so long as state laws provide equivalent or greater protection against discrimination, they are not preempted by federal law.[42] Yet the fairness guidelines imposed by Title VII, the ADA, and relevant state statutes are primarily limited to interview questions, questionnaires, and reference checks.[43] This has led state legislatures to create additional rules to constrain other pre-employment screening practices.

2. State Statutes Regulating Applicants' Arrest Records

In addition to self-reported information obtained through interviews, questionnaires, and references, employers often

35. *See* Befort, *supra* note 9, at 381 (citing Bruno v. City of Crown Point, 950 F.2d 355, 363–65 (7th Cir. 1991)).

36. *See id.* at 382 (citing EEOC, *Guide to Pre-Employment Inquiries*, 8A Fair Empl. Prac. Man. (BNA) 443:65–66 (1992)). Although EEOC guidelines do not have the force of law, courts generally give them considerable deference. *See* Griggs v. Duke Power Co., 401 U.S. 424, 433–34 (1997).

37. Americans with Disabilities Act, 42 U.S.C. §§ 12111–12117 (2006).

38. *See* Befort, *supra* note 9, at 383.

39. *Id.*

40. *See, e.g.*, CAL. GOV'T CODE § 12940 (West 2011); MINN. STAT. § 363A (2011); N.J. STAT. ANN. § 10:5-4 (West 2011).

41. MINN. STAT. § 363A.08, subd. 4(a)(1) (2011).

42. Befort, *supra* note 9, at 386.

43. *See id.* at 381–86.

conduct background checks to gather information on an applicant's criminal record.[44] Criminal background checks are usually permissible if employment decisions based on an applicant's criminal record are consistent with a business necessity and do not have a disparate impact on a certain class of applicants.[45] A number of states have also restricted or prohibited the use of arrest records, but not conviction records, in criminal background checks.[46] Because arrests do not necessarily establish guilt, these state statutes aim to avoid disparate impact problems while preventing the penalization of persons not subsequently charged with a crime for which they were arrested.[47] But since Title VII and the ADA provide the theoretical support for state restrictions on arrest records in the hiring context,[48] states have been reluctant to expand restrictions on pre-employment screening beyond criminal background checks. However, some states restrict employers' ability to look at other types of public records.[49]

3. The FCRA and Credit Scores

Many employers also screen applicants by examining credit reports compiled by consumer credit reporting agencies.[50] Using statistical formulas that reflect an individual's bill-paying history, including late collection actions, consumer credit re-

44. *See id.* at 404–06.

45. *See id.* at 404–05.

46. *See, e.g.*, CAL. LAB. CODE § 432.7 (West 2011); 775 ILL. COMP. STAT. 5/2-103 (2011); MICH. COMP. LAWS ANN. § 37.2205a (West 2011); N.H. REV. STAT. ANN. § 21-I:51 (2011); WASH. REV. CODE § 10.97.050 (2011); WIS. STAT. § 111.335 (2011). *See generally* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1169 (2002) ("Confronted with increased information trade, some states have attempted to restrict access to personal information in public records as well as certain uses of personal information obtained from public records.").

47. *See* Ecker, *supra* note 29, at 255–56.

48. *Cf.* Griggs v. Duke Power Co., 401 U.S. 424, 430–31 (1971) (holding that otherwise neutral selection devices that have a disparate impact on protected classes may violate Title VII).

49. *See* Solove, *supra* note 46, at 1169–70.

50. *See* Ecker, *supra* note 29, at 257. A survey released by the Society for Human Resource Management reveals that forty-seven percent of employers admit to using credit checks for certain job applicants. *Background Checking: Conducting Credit Checks*, SOC'Y FOR HUMAN RES. MGMT. (Jan. 22, 2010), http://www.shrm.org/Research/SurveyFindings/Articles/Pages/BackgroundChecking.aspx.

porting agencies generate a credit score.[51] Next, these third-party reporting companies sell the relevant credit reports to interested employers who demonstrate a legitimate business need for the information.[52] Employers may view an applicant's credit score as a proxy for trustworthiness, since higher credit scores are associated with creditworthiness and an ability to meet one's obligations.[53]

Thus, to avoid liability during the credit reporting process, both the employer and the third-party consumer credit reporting agency must comply with the FCRA. In 1970, Congress passed the FCRA to "require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information . . . ."[54] The FCRA gives the Federal Trade Commission (FTC) the primary administrative authority to enforce the provision of the FCRA.[55] According to the FTC, the FCRA is "intended to ensure that this country's consumer reporting system would function fairly, accurately, and efficiently, without needless intrusion into consumer privacy."[56] Courts generally agree that the purpose of the FCRA is to ensure accuracy in reports affecting an individual's eligibility for credit, insurance, or employment.[57]

The FCRA makes clear that applicants must give permission to an employer before a credit report is initiated,[58] and that notice must be given to applicants if an adverse decision results

51. *See Building a Better Credit Report*, FED. TRADE COMM'N, 3 (Aug. 2011), http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre03.pdf.

52. *See id.* at 1.

53. *See id.* at 3 ("[A credit score] helps predict . . . how likely it is that [a person] will repay a loan and make the payments on time.").

54. H.R. REP. No. 91-1587, at 16 (1970).

55. *See* Amanda L. Fuchs, Comment, *The Absurdity of the FTC's Interpretation of the Fair Credit Reporting Act's Application to Workplace Investigations: Why Courts Should Look Instead to the Legislative History*, 96 NW. U. L. REV. 339, 341 (2001).

56. *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the Comm. on Banking, Fin. and Urban Affairs*, 102d Cong. 20 (1991) (statement of David Medine, Associate Director for Credit Practices, Federal Trade Commission).

57. *See, e.g.*, D'Angelo v. Wilmington Med. Ctr., 515 F. Supp. 1250, 1253 (D. Del. 1981); Porter v. Talbot Perkins Children's Servs., 355 F. Supp. 174, 176 (S.D.N.Y. 1973) (citing 116 CONG. REC. 36,572 (1970)).

58. 15 U.S.C. § 1681b(b) (2006).

from the credit report.[59] Moreover, the consumer reporting agency, following a consumer's request, must disclose the information that it maintains in the consumer's file.[60] Violators of the FCRA can be sued for actual damages and, in some cases, punitive damages.[61]

Importantly, the FCRA only applies to "consumer report[s]" prepared by "consumer reporting agenc[ies]."[62] "Consumer report" is defined as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's . . . character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for . . . employment purposes.[63]

The FCRA defines a "consumer reporting agency" as any individual or business that "regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ."[64] Based on these broad statutory definitions, the FCRA applies to more than simply credit reports; other types of background checks are subject to the FCRA.[65] However, the statutory language noticeably fails to include informal research, performed without third-party assistance, from FCRA regulation.

4. The Fourth Amendment

A final constraint, specifically on government employers' pre-employment screening practices, is found in the Fourth Amendment. Many job applicants worry that pre-employment background checks—whether criminal, credit, or otherwise—are an invasion of privacy in violation of the Fourth Amendment.[66] Consequently, privacy in the workplace, including the

59. *See* 15 U.S.C. § 1681m (2006); Ecker, *supra* note 29, at 258.

60. 15 U.S.C. § 1681g(a) (2006).

61. 15 U.S.C. §§ 1681n–1681o (2006).

62. *Id.*

63. 15 U.S.C. § 1681a(d)(1) (2006).

64. 15 U.S.C. § 1681(f) (2006).

65. *See* Byrnside, *supra* note 3, at 465.

66. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

off-duty activity of job applicants, is garnering increased legal attention.[67]

Historically, Fourth Amendment violations were tied to property invasions by law enforcement.[68] But modern courts have expanded Fourth Amendment rights to protect reasonable expectations of privacy, following *Katz v. United States*.[69] Accordingly, job applicants frequently argue that pre-employment screening is an invasion of privacy.[70] Yet much of the information gathered by employers through traditional pre-employment screening tools is publically available, and the Fourth Amendment only applies to certain kinds of *governmental* intrusions, which severely limits the Fourth Amendment's application to pre-employment screening.[71] Nevertheless, the Fourth Amendment legitimizes an expectation of privacy in some circumstances.[72]

Title VII, the ADA, state statutes, the FCRA, and the Fourth Amendment provide a legal framework for traditional pre-employment screening practices. However, this regulatory structure is being challenged by social media, a tool that makes it easier and cheaper for employers to acquire applicant information.[73] Even though the use of social media as an information-gathering technique is increasing,[74] this new hiring practice has not met universal praise. In fact, distrust of social media in the hiring arena is abundant, evidenced by numerous

67. *See, e.g.*, Stephen D. Sugarman, *"Lifestyle" Discrimination in Employment*, 24 BERKELEY J. EMP. & LAB. L. 377, 378, 407 (2003) (discussing the privacy impact of different methods of pre-employment research).

68. *See, e.g.*, *In re* Pac. R.R. Comm'n, 32 F. 241 (C.C.N.D. Cal. 1887) (recognizing a citizen's fundamental right to security from government inspection of physical items such as private books and papers).

69. 389 U.S. 347, 360–62 (1967) (Harlan, J., concurring) (finding that the government violated the Fourth Amendment by conducting warrantless eavesdropping with an electronic listening device, because the defendant justifiably relied upon the privacy of a public telephone booth).

70. *See* Ecker, *supra* note 29, at 274.

71. *See Katz*, 389 U.S. at 350; Byrnside, *supra* note 3, at 452 ("Applicants . . . often seek the ability to control their off-duty conduct regardless of a reasonable expectation of privacy.").

72. *Compare* United States v. Mankani, 738 F.2d 538, 542 (2d Cir. 1984) (holding that the use of a beeper to track an individual's vehicular movements was not a search in violation of the Fourth Amendment), *with* Kyllo v. United States, 533 U.S. 27, 34 (2001) (deciding that the use of a thermal imager to detect the heat emanating from the defendant's home violated the Fourth Amendment).

73. *See* Byrnside, *supra* note 3, at 453.

74. *See id.*

news articles expressing outrage over social media's new role in pre-employment screening.[75] Before detailing social media's unique impact on pre-employment screening, it is necessary to review the history and characteristics of social media.

B. THE EMERGENCE OF SOCIAL MEDIA

Social media websites have exploded in popularity within the last several years, amassing millions of dedicated users.[76] Joining a social media community is easy. On Facebook, for example, a user, armed with an e-mail address, a full name, and a birth date, is quickly able to access an online community that grows larger by the day.[77] If Facebook were a country, it would be the third largest in the world, landing behind China and India but ahead of the United States.[78] Facebook provides a template into which a user, once registered, can enter virtually limitless information: relationship status, schools attended, favorite movies, e-mail addresses, home addresses, and more.[79] Members may also post photos online with a "tag" that identifies the people in the photo by name and adds the photo to those users' personal profiles.[80]

The breadth of personal information uploaded to social media websites raises concerns over who can see what information and when. While Facebook allows members to restrict the availability of the information posted online, the content is less private than many users believe.[81] Facebook's default privacy settings are at a level intended to maximize visibility of user profiles and to increase privacy the user must sort through

75. *See, e.g.*, Alan Finder, *For Some, Online Persona Undermines a Résumé*, N.Y. TIMES, June 11, 2006, at 1; Ken Rodriguez, *Want a Job After Graduation? Don't Reveal Your Wild Side Online*, SAN ANTONIO EXPRESS-NEWS, July 5, 2006, at 3A.

76. *See, e.g.*, Samantha L. Millier, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 544 (2008).

77. As of July 21, 2010, 500 million users were registered on Facebook. Mark Zuckerberg, *500 Million Stories*, THE FACEBOOK BLOG (July 21, 2010, 9:23 AM), http://blog.facebook.com/blog.php?post=409753352130.

78. *See* Brian Solis, *Facebook Connects 500 Million People: Defines a New Era of Digital Society*, BRIANSOLIS.COM (July 22, 2010), http://www.briansolis.com/2010/07/facebook-connects-500-million-people-defining-a-new-era-of-digital-society/.

79. Millier, *supra* note 76, at 544.

80. John Cassidy, *Me Media: How Hanging Out on the Internet Became Big Business*, NEW YORKER, May 15, 2006, at 50.

81. *See* Byrnside, *supra* note 3, at 460–61.

somewhat complicated (not to mention constantly changing)[82] option menus.[83] Privacy advocates are especially wary of Facebook and other social media platforms.[84] By making online content permanent and widespread, social media creates digital baggage that can be hard to escape.[85] Furthermore, third parties are free to post private and misleading information or images online without the user's consent.[86] In sum, Facebook users in particular, and social media users in general, have a false sense of security regarding the privacy of their social media profiles.[87]

The FTC is beginning to respond to these mounting concerns. For example, Facebook and the FTC have recently finalized a settlement over deceptive practices related to privacy settings.[88] The settlement requires Facebook to agree to privacy audits for twenty years and will prohibit Facebook from making public a piece of information that a user had originally shared privately on the site.[89] Nonetheless, the actual impact of the deal is unclear. Jeff Chester, the executive director of the Center for Digital Democracy, warns that the FTC's Facebook deal may only amount to "a tiny digital bump on the road that does nothing to derail [Facebook's] voracious appetite to swallow up our data."[90]

Employers have taken note of social media and its potential value as a hiring tool for precisely the same reasons that

82. *See, e.g.*, *The Evolution of Facebook Privacy*, YALE J.L. & TECH. (Apr. 21, 2011), http://www.yalelawtech.org/control-privacy-technology/evolution-of-facebook-privacy/.

83. *See* Byrnside, *supra* note 3, at 461.

84. *See generally* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 62 (2009) (arguing that social networking sites are breeding grounds for civil rights abuses).

85. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 10–11 (2007) (advocating for a new system of privacy on the Internet in order to address the challenges of digital rumors, gossip, and shaming).

86. *See* Millier, *supra* note 76, at 545.

87. Ira Nathenson, *Facebook: Job-Hunting, Non-Invisibility, and the Creepiness Factor*, NATHENSON'S DIGITAL GARBAGE (June 12, 2006), http://digitalgarbage.net/2006/06/12/facebook/; *see also* Tim Armstrong, *Social Darknets*, INFO/LAW (June 12, 2006), http://blogs.law.harvard.edu/infolaw/2006/06/12/social-Darknets/ (describing the mismatch between perceived privacy and the actual level of privacy enjoyed by social media users).

88. *See* Claire Cain Miller, *F.T.C. Said to Be Near Facebook Privacy Deal*, N.Y. TIMES, Nov. 11, 2011, at B3.

89. *See id.*

90. *Id.*

applicants and the FTC raise privacy concerns about its use; social media makes large amounts of previously unobtainable personal data readily accessible.[91] Indeed, social media "create[s] huge new portals for the mass disclosure of private information."[92] Thus, because of its novelty and informality, the use of social media in pre-employment screening escapes many of the regulations imposed on more traditional research techniques.

C. SOCIAL MEDIA AS A PRE-EMPLOYMENT SCREENING TOOL

Companies are rapidly adding social media pre-employment screening to their hiring playbooks. Tech giant Microsoft admits that "researching students through social networking sites [is] now fairly typical."[93] Likewise, according to a study conducted by CareerBuilder.com, about twelve percent of hiring managers screen job candidates by searching profiles on social networking sites.[94] The actual number of employers screening applicants over the Internet is probably higher, and sometimes large companies may not even be aware that those involved with hiring decisions are researching applicants online and factoring online information into their evaluations.[95] Even some professional associations are using social media during background investigations. The Florida Bar Association Board of Bar Examiners visits Facebook and MySpace to investigate the "good moral character and fitness" status of bar applicants.[96]

91. *See* Byrnside, *supra* note 3, at 455.

92. Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 890 n.16 (2006).

93. Byrnside, *supra* note 3, at 456 (alteration in original) (citing Alan Finder, *When a Risque Online Persona Undermines a Chance for a Job*, N.Y. TIMES, June 11, 2006, at 1).

94. *See One-in-Four Hiring Managers Have Used Internet Search Engines to Screen Job Candidates; One-in-Ten Have Used Social Networking Sites, CareerBuilder.com Survey Finds*, CAREERBUILDER.COM (Oct. 26, 2006), http://www.careerbuilder.com/share/aboutus/pressreleases.aspx (follow "2006" hyperlink; then follow "10/26/2006" hyperlink).

95. *See* Michelle Sherman, *Legal Issues Surrounding Social Media Background Checks*, FCPA COMPLIANCE & ETHICS BLOG (Nov. 17, 2011, 1:13 AM), http://tfoxlaw.wordpress.com/2011/11/17/.

96. *See* Jan Pudlow, *On Facebook? FBBE May Be Planning a Visit*, THE FLA. BAR NEWS (Sept. 1, 2009), http://www.floridabar.org/DIVCOM/JN/jnnews01.nsf/8c9f13012b96736985256aa900624829/d288355844fc8c7285257619900652232?OpenDocument.

Unlike credit reports or criminal history background checks, employers usually research an applicant's social media profile without seeking the assistance of a third-party reporting company.[97] Employers run quick social media searches from a company or personal computer in hopes of finding informative online content.[98] But since September 2010, some employers across the nation are contracting with third-parties, like Social Intelligence, to institute formalized social media background checks.[99] The effect of this new development is significant: third-party reporting agencies must comply with the FCRA when performing social media research.[100] However, it is clear that many employers—if not most—continue to conduct informal social media screens.[101]

As a consequence of social media's popularity and accessibility, one might think that most job applicants would choose to remove, or not post, provocative online information that could reach an employer.[102] Numerous stories indicate otherwise. For example, one eager job applicant failed to receive an offer after being linked to an online advertisement seeking OxyContin.[103] Similarly, after discovering that an applicant's Facebook profile included interests such as "'smokin' blunts' . . . shooting people and obsessive sex," one employer removed an otherwise qualified applicant from consideration.[104] Even if such online behavior is in jest and taken out of context, employers are unlikely to hire an individual who demonstrates poor judgment online.[105]

Although job applicants themselves are frequently to blame for the harmful online material that influences an employer's hiring decision, the accuracy, authenticity and relevance of online content is suspect,[106] particularly because photo

97. *See* Byrnside, *supra* note 3, at 457 (positing that the majority of employers do not use formal means to research an applicant's online behavior).

98. *See* Melissa Bell, *More Employers Using Firms that Check Applicants' Social Media History*, WASH. POST, July 15, 2011, at C1 (discussing generally the ease with which employers can find details of applicants online).

99. *See id.*

100. *See* Mithal, *supra* note 15, at 1.

101. *See* Bell, *supra* note 98.

102. *See* Millier, *supra* note 76, at 542–43 (discussing the problem by which "the desire to share information with one's friends may also expose users to unknown third parties who may misuse their information").

103. Preston, *supra* note 1, at B1.

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

105. *See* Byrnside, *supra* note 3, at 473–74.

106. *See id.* at 470–71.

editing tools and hacking problems are ubiquitous.[107] In light of these concerns, together with the uniqueness and usefulness of social media from an employer's perspective, the question arises: is there a legal framework that can adequately regulate social media pre-employment screening?

II. THE UTILITY OF EXISTING REGULATORY SCHEMES AS APPLIED TO IN-HOUSE SOCIAL MEDIA PRE-EMPLOYEMENT SCREENING

The unique features of social media pre-employment screening make its use cumbersome to regulate under existing laws.[108] Unlike its predecessors, most social media pre-employment screening is performed in-house without third-party assistance.[109] Furthermore, social media screening is quick, convenient and anonymous. As a result, many employment attorneys conclude that there is nothing illegal about employers using social networking sites to research applicants.[110] And since a case has yet to arise that suggests otherwise, the potential liability risks to employers who use social media to screen applicants appear to be low.[111] Simply put, Title VII, the ADA, state statutes, the Fourth Amendment, and the FCRA do not adequately impose restrictions, or the threat of liability, on employers who informally screen job applicants with social media. These deficiencies, however, do not warrant wholesale abandonment of the regulatory principles that control traditional pre-employment screening practices. In particular, the Fourth Amendment and the FCRA promote useful notions of limited online privacy and notice that should be applied to social media pre-employment research.

A. THE SHORTCOMINGS OF TITLE VII AND THE ADA

An employer that refuses to hire an applicant due to the candidate's protected class status may violate the anti-

107. *See* Ian Lovett & Adam Nagourney, *Arrest Is Made in Hacking of Celebrities' Private E-Mail*, N.Y. TIMES, Oct. 12, 2011, at A20 (reporting that all computer users are vulnerable to hacker attack).

108. *See* Corey M. Dennis, *Legal Implications of Employee Social Media Use*, 93 MASS. L. REV. 380, 381–92 (2011) (discussing the risk of liability from invasion of privacy and discrimination claims).

109. *See* Byrnside, *supra* note 3, at 457.

110. *Hiring: Pitfalls of Checking Job Applicants' Personal Web Pages*, MANAGING ACCOUNTS PAYABLE, Oct. 2006, at 4, 5.

111. *See* Dennis, *supra* note 108, at 381 (acknowledging that the primary liability risk is from employment discrimination lawsuits).

discrimination principles of Title VII and the ADA. As indicated above, Title VII and the ADA forbid discrimination based on an applicant's race, color, religion, sex, national origin, or disability.[112] Social media profiles regularly display such sensitive information, in addition to other intimate details of users' private lives.[113] The availability of this information online does not necessarily lead to discrimination—only adverse employment decisions based on an applicant's social media profile could result in discrimination claims—but social media does provide employers a chance to access information they would otherwise not be privy to and certainly would be unable to ask about during a job interview.[114]

If an employer used social media to ascertain applicants' membership in a protected class and subsequently used that information to systematically remove certain applicants from employment consideration, the employer would risk liability for discrimination.[115] Assuming a claimant could provide documentation of the discriminatory practice, Title VII and the ADA would proscribe that sort of social media pre-employment screening.[116] Other discriminatory use of social media pre-employment screening could also implicate Title VII and the ADA—for example, if an employer only viewed the social media profiles of certain types of applicants, or if it viewed some social media content with a discriminatory lens.[117]

But Title VII and the ADA only go so far. The type of personal or misleading information collected by social media pre-employment screening is usually unrelated to race, religion, sex, disability, or any other protected class.[118] Employers turn to social media in an effort to learn all manners of personal information, "including drinking habits, nudity, general sleaziness, and criminal behavior ranging from shoplifting to violent

112. *See supra* discussion at Part I.A.1.

113. *See* Byrnside, *supra* note 3, at 462–63 (noting that users' sexual orientation, political affiliation, age, and marital status are commonly viewable on social media profiles).

114. *See id.*

115. *See* 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.

116. *See* Byrnside, *supra* note 3, at 463–64 (using the example of an employer who only looks at the profiles of African Americans and women).

117. *See id.*

118. *See* Dennis, *supra* note 108, at 381.

assaults."[119] It is exactly this kind of personal information that applicants argue should be excluded from pre-employment research.[120] Applicants want the freedom to express themselves online without fear that employers may find this information and then use it to make hiring decisions.[121] Applicants further contend that an employer's hiring decision should come down to who is best qualified for the job, not the applicant whose lifestyle choices resonate with, or least offend, an employer.[122] While anti-discrimination statutes play an important role in ensuring that social media sites are not used as an unfair hiring tool, Title VII and the ADA do not address the biggest problems of social media screening—authenticity, accuracy, and relevance.[123] Under both Title VII and the ADA, it appears to be perfectly legal for an employer to methodically exclude applicants with drunken or provocative photos on their social media pages.[124]

B. STATE STATUTES REGULATING BACKGROUND CHECKS ARE LIMITED IN APPLICATION

Adding to the protections of Title VII and the ADA, most states have enacted statutes that restrict or prohibit employers' inquires about an applicant's arrest record.[125] State legislatures were worried that even though an arrest is not an indication of guilt, employers would unfairly disqualify those applicants with arrest records.[126] On its face, social media screening shares many of the negative aspects inherent in employers' use of arrest records, as online content may be highly prejudicial and

119. LaJean Humphries, *The Impact of Social Networking Tools and Guidelines to Use Them*, LLRX.COM (Jan. 15, 2007), http://www.llrx.com/features/goodgoogle.htm.

120. *Cf.* Finder, *supra* note 75, at 3 (discussing students' views that the "adult world" does not know about social media sites such as Facebook).

121. *See* Byrnside, *supra* note 3, at 472.

122. *See* Dennis, *supra* note 108, at 382 (arguing that reference checks, interviews and more traditional background screening will satisfy most employers' need to hire the best candidate).

123. *See, e.g.*, *id.* ("[O]n social networking sites and blogs, destructive groups have published lies and doctored photographs of vulnerable individuals, sent damaging statements about victims to employers, and manipulated search engines to highlight those statements for business associates and clients to see.").

124. *See* Byrnside, *supra* note 3, at 465.

125. *See supra* discussion at Part I.A.2.

126. *See* Ecker, *supra* note 29, at 255.

entirely unrelated to an applicant's ability to perform job duties.[127]

Regardless of the similarities, state statutes pertaining to arrest records are not an appropriate foundation for regulating social media pre-employment screening. First, these state statutes are situation specific and do not provide a broad privacy or accuracy principle that can be applied to other forms of background research.[128] Even assuming that social media are the kinds of public records that states occasionally regulate, state statutes only limit access in predefined areas.[129] Indeed, the majority of public records are unrestricted.[130]

Additionally, expanding state regulations to include social media pre-employment screening ignores the advantages of a national policy. A strong national policy regarding social media background checks is preferable over widely differing state public record regimes because a national policy would create a minimum level of privacy protection.[131] A uniform privacy baseline increases the likelihood that applicants would know about their privacy rights, and likewise, that users of restricted information would know the responsibilities that accompany their access to such information.[132] Therefore, a federal baseline must be established; states would be free to adopt stricter protections of privacy, but a federal program "must provide a meaningful floor of protection."[133] While admirable in purpose, state statutes restricting employers' use of arrest records are not fully responsive to social media screening.

C. THE FOURTH AMENDMENT PROVIDES HELPFUL PRINCIPLES, BUT CASE LAW PREVENTS ITS APPLICATION TO SOCIAL MEDIA PRE-EMPLOYMENT SCREENING

Despite its frequent invocation, a Fourth Amendment invasion of privacy claim corresponding to employers' use of social media to screen applicants is unlikely to succeed. As a threshold matter: "[T]he Fourth Amendment cannot be trans-

127. *See* Dennis, *supra* note 108, at 381–82.

128. *See* Solove, *supra* note 46, 1169–70.

129. *See id.* (discussing context-dependent state statutes that restrict access to motor vehicle, accident, traffic citations, voter, and arrest records).

130. *See id.*

131. *Cf. id.* at 1200 (preferring a national over a state regulatory system for public records as technological advances increase the digitization of public documents).

132. *See id.*

133. *Id.*

lated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of *governmental* intrusion . . . ."[134] It follows that the Fourth Amendment cannot adequately regulate social media pre-employment screening since a substantial portion of employers—private employers—would elude its protections.

Further limiting an applicant's Fourth Amendment claim arising from social media pre-employment screening is the rule that a claimant must have a reasonable expectation of privacy in order to bring suit.[135] Critically, courts often consider information available online to be in the public domain,[136] and "the rule of thumb is: If it's in the public domain, it's fair game."[137] In other words, existing precedent indicates that a person who willingly posts personal information to a social media site lacks a reasonable expectation of privacy regarding that information.[138] In rare circumstances, however, an applicant might be able to assert a credible invasion of privacy claim against a government employer. For example, an applicant may have a strong invasion of privacy claim if the employer hacks past the privacy settings on an applicant's social media page, or if a third party unlawfully posted private information online.[139] But even stringent privacy settings do not guarantee a successful invasion of privacy claim following a breach. It would be "tough to prove that this expectation of limited access, even if reasonable, is an expectation of 'privacy.'"[140]

134. Katz v. United States, 389 U.S. 347, 350 (1967) (emphasis added).

135. *See supra* discussion at Part I.A.4.

136. *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 (2000) (discussing the availability of new legal developments that can be found online in considering whether to reprimand attorneys for professional conduct violations).

137. Martha Irvine, *Privacy Becomes Concern as Social Media Online Sites Become Fair Game*, USA TODAY (Dec. 30, 2006), http://www.usatoday.com/tech/news/2006-12-30-privacy-online_x.htm.

138. *See generally* John. S. Ganz, Comment, *It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices*, 95 J. CRIM. L. & CRIMINOLOGY 1325, 1333–34 (2005) (finding existing precedent to be critical of invasion of privacy claims that are based on publicly observable and voluntarily exposed information).

139. *See* George Lenard, *Employers Using Facebook for Background Checking, Part I*, GEORGE'S EMP'T BLAWG (Dec. 6, 2006), http://www.employmentblawg.com/2006/employers-using-facebook-for-background-checking-part-i/.

140. *Id.*

While the Fourth Amendment's direct extension to social media pre-employment screening is untenable, recent Fourth Amendment jurisprudence does provide a useful framework for thinking about privacy on the Internet. In the landmark decision *United States v. Maynard*, the court applied a "mosaic theory" to rule that prolonged and warrantless GPS vehicular surveillance amounted to a search in violation of the Fourth Amendment.[141] The court recognized a reasonable expectation of privacy regarding the totality of one's movements on public streets, even though isolated outings are publicly exposed.[142] For the court, a reasonable person expects that each public movement will remain "disconnected and anonymous."[143] Since *Maynard*, the mosaic theory has received praise in some circles for elegantly accommodating an expectation of privacy in some public activity.[144]

Building on the *Maynard* precedent, several scholars suggest that personal information, while public to an extent when posted on the Internet, demands some level of privacy protection. According to Professor Daniel J. Solove:

> Privacy involves an expectation of a certain degree of accessibility of information . . . . [P]rivacy entails control over and limitations on certain uses of information, even if the information is not concealed. Privacy can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible . . . .
>
> We know that our lives will remain private not in the sense that the information will be completely shielded from public access, but in the sense that for the most part, it will be lost in a sea of information about millions of people. Our personal information remains private because it is a needle in a haystack, and usually nobody will take the time to try to find it.[145]

However, the fact remains that only a few courts, in limited situations, have been willing to abandon the public versus

141. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012). Since the U.S. Supreme Court affirmed the *Maynard* decision on slightly different grounds, the lasting impact of the mosaic theory remains to be seen.

142. *Id.*

143. *Id.* at 563 (quoting Nader v. Gen. Motors Corp., 25 N.Y.2d 560, 572 (1970) (Breitel, J., concurring)).

144. *See, e.g.*, Bethany L. Dickman, Note, *Untying* Knotts*: The Application of Mosaic Theory to GPS Surveillance in* United States v. Maynard, 60 AM. U. L. REV. 731, 738 (2011).

145. Solove, *supra* note 46, at 1178. *Contra* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010) ("[W]hen Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others.").

private dichotomy that defeats a reasonable expectation of privacy if the contested information is disclosed publicly.[146] Still, the novel efforts by some courts to include seemingly public information under the Fourth Amendment legitimize the regulation of social media pre-employment screening. Sure, social media sites are in the public domain, but their use—especially by employers—should not be without limits.

D. THE FCRA: A WORKABLE BUT INSUFFICIENT BASIS FOR REGULATING SOCIAL MEDIA'S PROMINENCE IN HIRING DECISIONS

As argued above, social media pre-employment screening should be regulated not with the goal of preventing it, but rather to control accessibility and ensure authenticity, accuracy, and relevance.[147] To that end, the FCRA contains the procedural requirements necessary to regulate social media pre-employment screening in a manner that responds to the privacy values expressed in recent Fourth Amendment jurisprudence. Under the FCRA, an employer must (1) receive an applicant's permission before a background check is conducted and (2) notify the applicant if an adverse employment decision is based on the background check.[148] Applying these requirements to social media pre-employment screening sufficiently protects applicants' privacy interests without unduly harming employers' "best fit" concerns.

First, by requiring prior approval, the FCRA ensures that applicants will not be surprised when an employer views social media content. Relatedly, prior approval gives the applicant an opportunity to clean up potentially misleading information,

146. *See* Solove, *supra* note 46, at 1181–82. *Compare* Y.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d 488, 502 (Mo. Ct. App. 1990) (holding that plaintiffs did not waive their right to keep their participation in a medical program private by attending a party for those involved in the program), *and* Sanders v. Am. Broad. Co., 978 P.2d 67, 72 (Cal. 1999) (recognizing a reasonable expectation of privacy in workplace discussions with coworkers even though others could overhear the conversations), *with* Nader v. Gen. Motors Corp., 255 N.E.2d 765, 770 (N.Y. 1970) (ruling that personal information already disclosed to others could hardly be considered private despite the fact that it had been shared with select persons only), *and* Fisher v. Ohio Dep't of Rehab. & Corr., 578 N.E.2d 901, 902 (Ohio Misc. 2d 1988) (determining that a plaintiff who told four coworkers that some interactions between herself and her young son had "sexual overtones" could claim no reasonable expectation of privacy as to her statements).

147. *See supra* discussion at Part II.C.

148. *See supra* text accompanying notes 50–53.

prepare explanations regarding suspicious material or increase privacy settings on particular content. If "claims that employers are invading applicants' privacy by looking at their social networking profiles [are] the most common,"[149] then giving an applicant notice rewards the attentive applicant and dissociates social media pre-employment screening from a form of online spying.

Second, by requiring notice for adverse decisions based on a social media pre-employment screen, the FCRA affords an applicant another opportunity to correct or remove damaging online content. It may be easy to blame an applicant for sexually explicit photos posted on the Internet, but as more people post content online and do so at a much younger age, a disparaging comment or activity could be essentially forgotten until uncovered by the employer. As noted by attorney Ian Byrnside, "[w]here 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."[150] Furthermore, this disclosure would create a formalized record of the online content, a potentially useful tool in Title VII or ADA litigation.

Compared to other regulatory options, it is unlikely that employers would be unduly burdened by FCRA-regulated social media pre-employment research. Instead of completely banning social media from playing a role in hiring decisions, the FCRA would allow employers to access pertinent online content as it relates to future job performance.[151] The FCRA gives employers a choice: conduct social media research the right way—in a way that actually maximizes legally permissible applicant data—or not at all. Undoubtedly, contracting with a third party to conduct social media screens would be more expensive and would require more planning than in-house research, but it is possible that the efficiency gains due to a condensed and relevant third-party report would more than make up for the employer's monetary investment.[152] Employers could also prioritize which vacant positions were important enough to require social media

149. Byrnside, *supra* note 3, at 461.

150. *Id.* at 476 (quoting *Your Resume May Be Overshadowed by Your Online Persona*, PRIVACY RTS. CLEARINGHOUSE (July 9, 2006), http://web.archive.org/web/20110708005601/https://www.privacyrights.org/print/ar/OnlinePersona.htm).

151. *See* 15 U.S.C. §§ 1681–1681t (2006).

152. For Social Intelligence's list of the advantages of third-party reporting, see SOCIAL INTELLIGENCE, http://www.socialintel.com (last visited Oct. 18, 2012).

screening. And if all employers used third-party reports, a market would be created in which third-party reporting agencies would compete with each other for business, resulting in better services at lower prices.[153]

Unfortunately, the FCRA's significant merits do not change the fact that much of social media pre-employment screening is conducted by the employer, not a third-party screening company. No complex statistical formulas or detailed comparison factors are needed to understand an applicant's social media page.[154] Unless Facebook and similar social media websites revert back to a college-only admissions policy, an incredibly unlikely occurrence considering the success of expanded membership programs,[155] employers are not *forced* to go through third-party organizations to obtain social media content. And since the FCRA only impacts background research conducted by a third-party "consumer reporting agency," in-house research need not be FCRA compliant.[156] Thus, the employer does not have a legal duty to obtain permission prior to an investigation, provide notice of negative online information, or investigate potential errors and correct misinformation.[157]

However, the missing link capable of placing social media pre-employment screening under the FCRA umbrella is now a reality. Third-party social media screening and the corresponding FCRA compliance, provided by companies like Social Intelligence, is on the rise. That is a good thing for applicants. Still, employer participation in third-party screening is lacking, illustrating the need for FCRA tweaking.

153. *See* Hon. Richard D. Cudahy & Alan Devlin, *Anticompetitive Effect*, 95 MINN. L. REV. 59, 101–02 (2010) ("[P]erfect competition yields allocative and productive efficiency in the long run, while monopoly results in deadweight loss and wealth transfers.").

154. *See Building a Better Credit Report*, *supra* note 51, at 3.

155. *See* Press Release, Facebook, Facebook Expands to Include Work Networks (May 3, 2006), *available at* http://newsroom.fb.com/News/Facebook-Expands-to-Include-Work-Networks-d9.aspx.

156. 15 U.S.C. § 1681(f) (2006).

157. *Your Resume May Be Overshadowed by Your Online Persona*, PRIVACY RTS. CLEARINGHOUSE (July 9, 2006), http://web.archive.org/web/20110708005601/https://www.privacyrights.org/print/ar/OnlinePersona.htm.

III. THE FCRA AND THIRD-PARTY REPORTING: A FAIR WAY TO REGULATE SOCIAL MEDIA BACKGROUND CHECKS

Until very recently, social media pre-employment screening occurred in-house instead of through a third-party reporting agency.[158] Although employers regularly turned to third-party reporting agencies for criminal background checks or credit reports, the accessibility of social media encouraged employers to perform their own Internet research. To address the privacy implications of in-house social media research, previous scholarship advocated a "grandmother rule," where social media users would only post online content they would be comfortable sharing with their grandmas.[159] Likewise, employers were encouraged to forgive online youthful transgressions, or alternatively, merely avoid violating the restrictions of Title VII, the ADA, state statutes, and the Fourth Amendment when using social media.[160] Until a judicial or legislative decision was made regarding employers' use of social media in the hiring process, these solutions largely relied on the goodwill of employers to protect applicant data, a steep request considering the ease of online research.

But now, employers have the option to hire third parties to conduct social media pre-employment research. Since the FTC mandated that third-party social media screens must comply with the FCRA, all of the privacy and notice advantages of FCRA regulated pre-employment research (like credit reports) can be applied to the social media context. Nonetheless, simply the *option* to use third-party social media screening is not enough to protect applicant privacy or to ensure that employers will enjoy the advantages of third-party screening. If social media is to be considered during pre-employment evaluation, employers must be required to use third parties. Therefore, the FCRA should be amended to expressly prohibit in-house social media research. Like with other violations of the FCRA, a successful claimant should be permitted to recover damages from an employer who conducts in-house social media screens.

158. *See* Byrnside, *supra* note 3, at 465–66.
159. *See, e.g.*, *id.* at 474.
160. *See, e.g.*, *id.* at 474–76.

A. THIRD-PARTY SOCIAL MEDIA REPORTS WOULD PROTECT APPLICANT PRIVACY

As explained above, the FCRA has the potential to nicely regulate social media pre-employment screening by restricting, rather than prohibiting, Internet research.[161] FCRA-compliant social media screening puts the applicant on notice, giving him or her ample time to increase privacy settings, remove misleading information, or prepare explanations for suspicious online content.[162] Furthermore, it eliminates the guesswork from social media screening. No longer will applicants be forced to wonder whether it was their qualifications or spring break picture that removed them from job consideration. Any impact that social media pre-employment screening has on an employment decision must be reported to the applicant. This transparency decreases the likelihood of Title VII or ADA violations and allows an applicant to take remedial measures.[163]

At the same time, third-party social media reporting does not substantially harm employers. Personal information on the Internet is abundant, but as spokeswoman for the Society for Human Resource Management Jen Jorgensen correctly recognizes, "[j]ust because the information's out there doesn't mean it's useful."[164] Third-party reporting agencies can present employers with applicant information that is job-related and those agencies can remove sensitive information that could lead to disparate impact claims.[165] Additionally, because the FCRA imposes a duty to report accurate information, the likelihood that false or misleading social media content influences an employer's decision-making process will be reduced.[166] Familiarity with social media should allow third-party reporting agencies to better detect when particular content is the result of high-tech sabotage.

For some employers, however, even the benefits of more reliable social media data may pale in comparison to the costs of third-party social media reporting. Given that there are currently few legal risks associated with in-house social media

161. *See* discussion *supra* Part II.D.

162. *See supra* notes 128–30 and accompanying text.

163. *See* Byrnside, *supra* note 3, at 469–70.

164. *Id*. at 470 (citing H.J. Cummins, *Bosses Peek in on Web Site for Students*, SEATTLE POST-INTELLIGENCER, Apr. 3, 2006, at D1).

165. *See id.*

166. *See id.* at 471.

screening,[167] employers may be reluctant to give up in-house research for third-party social media screening. Yet these complaints fail to recognize that regulating social media pre-employment research with the FCRA would not require employers to hire third-party reporting agencies.[168] Employers would be free to forego social media research if the expense of third-party reporting were too great. And all of the traditional pre-employment screening tools—interviews, reference checks, criminal history reports—would still be available at little expense to the employer.[169] The substantial privacy interests implicated by in-house social media research outweigh the costs incurred by employers if they *choose* to pursue third-party social media pre-employment screening.

In addition to the benefits of FCRA compliant third-party social media research from an applicant's perspective—and its minor impact on employers—third-party social media screening is also consistent with the purpose of the FCRA. Congress enacted the FCRA to prevent "needless intrusion into consumer privacy" and to "ensure that this country's consumer reporting system would function . . . accurately."[170] Third-party reporting balances those legislative interests—it filters out irrelevant applicant information, it notifies the candidate of an employer's intention to conduct research over the Internet, and it provides the employer with accurate data. Social media's prominent role in hiring decisions was surely beyond the anticipation of Congress when the FCRA was first passed, but third-party social media screening is consistent with the fairness guidelines of the FCRA. Finally, it is important to note that the broad language and purpose of the FCRA provides a malleable legal standard that is able to keep pace with technological advancements. After all, future pre-employment screening practices will likely involve the Internet, but whether Facebook and Twitter will still be useful is anyone's guess.

Privacy commentators are beginning to take note of the advantages of third-party social media pre-employment screening. To test the third-party reporting process, Mat Honan, a

167. *See supra* note 110 and accompanying text.

168. *See supra* discussion at Part II.D.

169. *Cf.* Befort, *supra* note 9, at 415–16 (noting that several traditional pre-employment screening techniques are not overly expensive).

170. *Fair Credit Reporting Act: Hearing Before the Subcomm. on Consumer Affairs and Coinage of the Comm. on Banking, Fin. and Urban Affairs*, 102d Cong. 20 (1991) (statement of David Medine, Associate Director for Credit Practices, Fed. Trade Comm'n).

writer for the tech blog Gizmodo, along with five other Gizmodo employees, underwent a social media screen conducted by Social Intelligence.[171] The five others passed, but Mr. Honan's screen was more troublesome; online information revealed his previous proclivity for cocaine and LSD.[172] Despite the results, Mr. Honan concluded that "these kind of [third-party reporting] services actually make a lot of sense. . . . [I]t's better for both the employer and the candidate to have a disinterested third-party do full-scrape background checks."[173] Plus, the procedure may not be as invasive as one might think.[174] Anything that could be considered discriminatory or irrelevant in a job search was removed from Social Intelligence's final report.[175]

Nevertheless, third-party social media screening elicits comparisons to Big Brother.[176] A fear that mostly innocent Internet activity, including "bawdy jokes" or "slightly irreverent" photos,[177] will unfairly prevent qualified applicants from securing jobs drives much of the opposition to third-party social media reporting. Privacy-focused senators Al Franken and Richard Blumenthal recently wrote Social Intelligence to voice their concerns about "numerous scenarios under which a job applicant could be unfairly harmed by the information [Social Intelligence] . . . provides to an employer."[178] While well-intentioned, these criticisms miss the point. Employers, with or without disinterested third-party assistance, will research job applicants online. But by turning to companies like Social Intelligence, employers actually agree to submit to the fairness and accuracy requirements of the FCRA. As Mr. Honan points out, "[a]s an

171. *See* Mat Honan, *I Flunked My Social Media Background Check. Will You?*, GIZMODO (July 7, 2011, 2:13 PM), http://gizmodo.com/5818774/this-is-a-social-media-background-check.

172. *See id.*

173. *Id.*

174. Bell, *supra* note 98.

175. *See* Honan, *supra* note 171.

176. *See, e.g.*, *"Social Intelligence" Receives FTC Approval to Archive Facebook Posts for Job Screening Purposes*, FACECROOKS (June 22, 2011, 8:15 AM), http://facecrooks.com/Internet-Safety-Privacy/&E2%80%9CSocial-Intelligence%E2%80%9D-receives-FTC-approval-to-archive-Facebook-posts-for-Job-Screening-Purposes.html.

177. *Id.*

178. Letter from Sen. Al Franken & Sen. Richard Blumenthal, to Max Drucker, Chief Exec. Officer, Social Intelligence Corp. (Sept. 19, 2011), *available at* http://www.norwalkplus.com/nwk/information/nwsnwk/publish/News_1/Blumenthal-Franken-quiz-Social-Intelligence-Corp-on-practices_np_14566.shtml.

employee, you don't want potential employers knowing certain things about you that might make you a less attractive candidate due to their personal biases. As an employer, even if none of those things matter, just accidentally finding them out can be a problem."[179] Third-party social media reporting allows a neutral entity to determine what online content is appropriate during hiring considerations.

Questions regarding the privacy benefits of third-party social media pre-employment screening endure, perhaps because of the discomfort that typically attaches to new hiring practices.[180] Amidst this contentious environment, the FTC approved Social Intelligence's reporting practices as consistent with the FCRA.[181] After determining that Social Intelligence was indeed a consumer reporting agency under the FCRA, the FTC dropped its investigation into Social Intelligence's practices and thereby tacitly endorsed Social Intelligence's screening methods.[182] As long as the FTC continues to monitor the activities of Social Intelligence and other third-party screening companies, their implicit approval of third-party reporting is reasonable and actually respects applicant privacy.

The FTC's approval of Social Intelligence should increase employers' comfort with third-party social media reporting.[183] However, in order for the real benefits of third-party social media screening to be realized, more than just a handful of employers must seek the assistance of outside vendors.

B. SUGGESTIONS FOR MANDATING THIRD-PARTY SOCIAL MEDIA REPORTS

For the FCRA to have any force, employers that desire applicants' social media information must be required to hire third-parties to conduct their social media pre-employment screening. While the benefits of third-party social media reporting may incentivize some employers to forego in-house Internet research,[184] the additional expense may be enough to dissuade

179. *See* Honan, *supra* note 171.

180. *See* Kashmir Hill, *Senators Worried Job Seekers 'Unfairly Harmed' by Social Media Background Checks*, FORBES.COM (Sept. 20, 2011, 3:31 PM), http://www.forbes.com/sites/kashmirhill/2011/09/20/senators-worried-job-seekers-unfairly-harmed-by-social-media-background-checks/.

181. *See* Mithal, *supra* note 15, at 2.

182. *See id.*

183. *See* Sherman, *supra* note 95.

184. *See* discussion *supra* Part II.D.

many others. Therefore, the FCRA should be expanded to prohibit in-house social media research, federal agencies should strictly enforce third-party social media reporting, and employers should implement policies that prohibit internal screening.

Perhaps the best place to add a restriction on social media research would be in § 1681b of the FCRA since it deals with the permissible purpose of consumer reports. Following the discussion of the conditions for furnishing and using consumer reports for employment purposes,[185] clear language—mirroring the existing style of the FCRA—should be inserted that states: "Due to the increasing amount of personal data present on the Internet, there is a need to protect the consumer's right to privacy regarding such information. Subject to the requirements of this title, employers seeking information regarding a consumer's Internet presence, including, but not limited to, a consumer's social media activities, shall exclusively rely on consumer reporting agencies to supply such information." Obvious interpretation challenges would arise because of the terms "Internet presence" and "social media activities." Confusion could be mitigated by FTC guidance, however, and modifications to this proposed statutory amendment would be more than welcome. Political pressures, expert testimony, and enforcement feasibility would likely impact the language of the final amendment. What is important, though, is that employers are clearly prohibited from conducting in-house social media research, and held liable for noncompliance under § 1681n of the FCRA.

To add teeth to this proposed amendment, appropriate federal agencies must support properly conducted third-party social media reporting. By dropping its investigation of Social Intelligence, the FTC legitimized third-party social media screening.[186] More is needed. The FTC must not only regulate third-party reporting agencies, but it must also ensure that employers are discontinuing their reliance on informal social media searches. To do so, in accordance with its regulatory authority,[187] the FTC should regularly investigate employers that perform in-house social media research. When appropriate, the existence of an investigation should be identified in a press release. Additionally, the FTC should create and enforce harsh

185. *See* 15 U.S.C. § 1681b (2006).

186. *See supra* text accompanying notes 153–55.

187. *See* 15 U.S.C. § 45 (2006).

penalties for businesses that continue to informally mine social media for applicant data.[188]

The EEOC should partner with the FTC to address the problem of employers avoiding FCRA compliance by conducting informal social media research. Through its outreach, education, and technical assistance programs, the EEOC should highlight the benefits of third-party Internet screening. This support should not equal blind endorsement. Rather, the EEOC and FTC should recognize that third-party reporting that is *compliant* with the FCRA is the better alternative to in-house social media research.

Employers should take an active role too. Adopting an internal policy that prohibits in-house social media screening is a critical first step toward mandating third-party social media reporting. By incorporating a social media policy into an ethics and compliance program, employers can ensure that current employees involved in hiring decisions do not give in to the temptation to conduct informal Internet research.[189] And because employees cannot "un-see" content posted to social media pages—perhaps giving irrelevant information relevance during a hiring decision—employers should firmly prohibit in-house social media research.

Admittedly, informal use of social media is difficult to completely separate from hiring decisions. Even the staunchest advocate of third-party reporting may have a personal Facebook account that allows incidental contact with an applicant. Googling an applicant is unlikely to disappear. Ultimately, it is up to the applicant to make sure that all sensitive material is protected. And of course, states may impose tighter restrictions on social media reporting than those supplied by the FCRA. But in combination with third-party reporting, the FCRA works where other regulations have not, it already exists and it balances the competing interest involved in social media preemployment screening. Why reinvent the wheel?

CONCLUSION

The emergence of social media provides employers an opportunity to research applicants online. Due to low privacy settings and easy accessibility, employers routinely view applicants' social media pages during the hiring process. This upsets

188. *See id.*

189. *See* Sherman, *supra* note 95.

many job applicants. Even though such material is somewhat public, social media users are uncomfortable with the idea that online content that is possibly false, misleading, or irrelevant will play a role during hiring decisions. Previous efforts to control social media pre-employment screening and protect applicant privacy focused on Title VII, the ADA and the Fourth Amendment. However, these efforts were largely unsatisfactory. So long as employers did not violate a specific law, they had significant leeway to conduct social media research.

Beginning in 2010, third parties started offering to screen applicants online for interested employers. Third-party social media pre-employment screens are subject to the fairness constraints of the FCRA, and therefore they are a better solution to the privacy interests implicated by social media research. The FCRA requires applicant permission before a pre-employment screen may begin, gives an applicant notice of adverse decisions based on social media, and allows applicants to take remedial measures if their social media content is getting in the way of job opportunities. FCRA compliant third-party screens also ensure that employers receive only job-related information, adding efficiency to the hiring process. Consequently, the FCRA should be amended to require all employers interested in using social media to evaluate job applicants to use third-party screening companies. The FTC and the EEOC should be the primary parties responsible for enforcing employers' commitment to third-party social media pre-employment screening.