THE REFERENCES OF THE TWENTY-FIRST CENTURY: REGULATING EMPLOYERS' USE OF SOCIAL NETWORKING SITES AS AN APPLICANT SCREENING TOOL

Cara R. Sronce*

I. INTRODUCTION

Once upon a time, there existed a simple process for job-hunting. The process generally began with an application or resumé submission, and then employers arranged interviews with the applicants who provided the information best suited for, and most relevant to, that particular employer's needs. For some interviews there were dinners and drinks, and for others, twenty minutes and a handshake in the break room would suffice, but that was generally the extent of the investigation into the personality of applicants. Aside from checking in with the occasional reference, most offers of employment were made based on the applicants' qualifications on paper and their ability to remain composed enough during the interview to present a real fit with the company.

But hiring practices are evolving. The inception of the Internet opened the information floodgates, and it was not long before employers had access to more applicant information than just that found in the phone book. Employers could actually "google" someone to gather a host of information available through newspaper articles, websites, and online discussion boards.[1] Even so, at the time of Google's launch, the Internet was still a device for gathering information—for clicking a link to search and obtain.

Now, over ten years later, with the advent of the social networking site ("SNS"), the Internet has seen a shift from information-gathering to information-sharing. Now employers have access to large amounts of applicants' personal information that applicants themselves make available online to share with their friends. Websites such as Myspace, Facebook,

---

* Candidate for Juris Doctor at Southern Illinois University School of Law, May 2011. I would like to thank my mother, Robin Sronce, a first-rate researcher who has frequently shown me the value of putting one's own big ideas in writing. Also, many thanks to Alysha Schertz for entertaining the numerous conversations that propelled this topic forward, and the countless others that are sure to come.

1. The Google search engine even became its own verb. *Google History*, GOOGLE, http://www.google.com/intl/en/corporate/history.html (last visited Mar. 17, 2011).

and Twitter invite users to post personal information online in the form of a "profile," a place where they can also share pictures, videos, and any other piece of information they want. While this phenomenon is popular among the teenagers of the world, with 65 percent of online teens sharing information via social networking, studies show that adults are also engaging in online-sharing. Currently, 75 percent of online adults ages 18-24 and 35 percent of all adults participate in SNSs.[2]

While SNSs are fantastic tools to help individuals reconnect with friends and family or to promote a business or hobby, their positive utility is somewhat burdened by problems they can cause users. These include privacy issues that can arise when hosts sell user information or when sexual predators gain personal and detailed information about unsuspecting victims, or—the focal point of this Comment—when employers use the websites to check the backgrounds of job applicants. For the first time ever, employers may look beyond what applicants present in their resumes, references, and interviews; now, they may actually screen applicants based on the information gathered from browsing an applicant's online personality. And employers are taking full advantage of these opportunities. Recent studies show that 40-50 percent of employers are now using social networking websites in formulating a decision about job applicants, a figure that is continually increasing.[3]

Because of the many concerns surrounding SNS technology use by employers, some legal scholars advocate laws to regulate employers' use of social networking sites.[4] In light of the current discourse on this subject, this Comment examines whether there should be a law, similar to the Fair Credit Reporting Act (FCRA), requiring employers to notify applicants if they are denied employment based on information found on their social networking profile. This discussion begins in section II with the background of the issue, highlighting the concerns arising from hiring practices involving SNSs, followed by a look into the current case law dealing with employers' use of these websites in general. Next, section III

---

2. Amanda Lenhart, *Adults and Social Network Websites*, PEW INTERNET (Jan. 14, 2009), http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites/1-Summary-of-findings.aspx.

3. These figures vary depending on which study is used. An article in the New York Times featured a study conducted by Harris Interactive for Careerbuilder.com, which found 45 percent of employers questioned are using social networking sites to screen applicants. *See* Jenna Worthham, *More Employers Use Social Networks to Check Out Applicants*, N.Y. TIMES (Aug. 20, 2009, 3:27 PM), http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/.

4. Donald Carrington Davis, *Myspace Isn't Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services*, 16 KAN. J.L. & PUB. POL'Y 237 (2007).

will examine the principal proposed solution to this problem, and finally section IV will promote an alternate solution that does not hinge on expanding the FCRA. Ultimately, this Comment argues that the FCRA should not be expanded to include information found on SNSs, but some disclosure of these hiring practices is necessary.

II. BACKGROUND

In order to determine whether expanding the Fair Credit Reporting Act is the appropriate solution, it is important to first understand the fears driving the push for new legislation regulating SNSs. Accordingly, this section presents the major problems for both applicants and employers that arise from the lack of employer regulation in this area. Next, it takes a detailed look at the proposal to expand the FCRA.

A. Concerns Over the Use of Social Networking Media in Hiring

There are many concerns for both applicants and employers about the use of social networking media by employers, indicating that employers are in need of protection to the same extent as are their applicants. On one hand, applicants are suddenly accountable for not only their participation in the work environment, but also anything that they do on their personal time that may manifest itself on one of these websites. They also face the possibility of employers mistaking them for someone else or misunderstanding information found online. Yet, on the other hand, the consequences for employers are almost equally as serious and do not end at simple negligent hiring charges, but also extend to liability for discrimination, and in extreme cases, even human rights violations.[5] The following section considers first these consequences for applicants, illustrated through the experience of one student applicant in particular, then the consequences for employers.

1. Implications for Applicants Using Social Networking Media

Tien Nguyen, a senior at UCLA, stopped wondering why employers were not extending him interviews once he followed a friend's advice and

---

5. *See* John Naylor, *Online Social Networking: The Employers Dilemma*, CSM WIRE, 4, http://www.cmswire.com/images/WSS_whitepaper_socialnetwoking_legal_A4_final.PDF (last visited Mar. 17, 2011). Employees in the United Kingdom who are dismissed on the basis of something found on their social networking site actually have a Human Rights violation claim to make. *Id.* Article 8 of the Human Rights Act of 1998 provides that everyone has a right to respect for privacy and home life. *Id.*

"googled" himself.[6] After he discovered and removed the internet visibility of a satirical essay he wrote entitled, "Lying Your Way to the Top," the interviews and offers finally began to flow.[7] Tien's situation is one that lies at the heart of the debate over hiring practices involving internet screening. SNSs are used mainly for recreation and pleasure, not business. Individuals post information, the utility of which is generally its entertainment value, and employers are able to view this information without any explanation or notice to the applicant. By doing so, employers may easily take the information out of context and, in turn, use that information to make judgments on the applicant's character, motivation, and professionalism. Nguyen may not have actually been lying his way to the top, but the average employer had no way to know that his essay was satire and not his advice to fellow students looking to get ahead.

Another problem with employers' use of SNSs hinges on whether they could even be sure the person whose profile they are searching is actually the applicant. For example, when using the search function on Facebook for a very common name, "John Smith," Facebook returns 210,000 profiles for individuals with that name or close variations of that name, thus opening the door for applicants to face rejection based on information that actually belongs to someone else. One proponent of regulating this practice takes this suspicion a step further, arguing that there are those who would use social networking media maliciously, including "profile poachers" who create fake profiles for individuals.[8]

Ultimately, however, what the applicants fear is loss of privacy: an intrusion into the home life, which employers formerly could not access. Proponents of regulating legislation observe the disconnect that occurs when employers intercept—and use as a foundation for hiring decisions—information that was intended for a specific audience. They fear such a practice cannot be legitimate until there is a system in place to protect applicants who may be rejected based on inaccurate or misunderstood information, which they have no opportunity to justify.[9] The fact employers also need protection from the risky venture of using this information to screen applicants also propels the appeal of government intervention.

---

6. Alan Finder, *When a Risqué Online Persona Undermines a Chance for a Job*, N.Y. TIMES, Jun. 11, 2006.
7. *Id.*
8. Davis, *supra* note 4. See *infra* note 20 and accompanying text for an actual account of the "profile poacher" phenomenon.
9. Davis, *supra* note 4, at 242.

2. Hazards for Employers Who Use Social Networking Media to Screen Applicants

The pitfalls for employers who participate in internet screening are perhaps more serious than the consequences for potential applicants. Employment discrimination is nothing to be trifled with, given the abundance of laws[10] aimed at preventing discrimination based on race, sex, religion, national origin, and physical disability.[11] What is alarming about some of these networking sites is that they often specifically display information which most employers would never ask for in an interview for fear of a discrimination charge. Consider the main information page on the average Facebook profile, for example. Seven of the eight categories listed under the "basic information" tab on the profile page disclose the very things that contribute to most employment discrimination claims.[12] Thus, it is almost counterintuitive that while most of the aforementioned laws are enforced and policed heavily by the Equal Employment Opportunity Commission, not one specifically deals with the use of the internet in hiring practices.[13] What propels the risk, however, is that employers admittedly engage in this practice. In fact one study showed that 63 percent of employers who use these websites to research applicants actually make decisions based on the information found there, despite how susceptible this

---

10. *Federal Laws Prohibiting Job Discrimination*, EQUAL OPPORTUNITY EMP. COMM'N, http://www.eeoc.gov/facts/qanda.html (last modified Nov. 21, 2009). These include:

> Title VII of the Civil Rights Act of 1964 (Title VII), which prohibits employment discrimination based on race, color, religion, sex, or national origin; the Equal Pay Act of 1963 (EPA), which protects men and women who perform substantially equal work in the same establishment from sex-based wage discrimination; the Age Discrimination in Employment Act of 1967 (ADEA), which protects individuals who are 40 years of age or older; Title I and Title V of the Americans with Disabilities Act of 1990, as amended (ADA), which prohibit employment discrimination against qualified individuals with disabilities in the private sector, and in state and local governments; Sections 501 and 505 of the Rehabilitation Act of 1973, which prohibit discrimination against qualified individuals with disabilities who work in the federal government; Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA), which prohibits employment discrimination based on genetic information about an applicant, employee, or former employee; and the Civil Rights Act of 1991, which, among other things, provides monetary damages in cases of intentional employment discrimination.

Id.

11. *Employment Discrimination*, CORNELL U. L. SCH., http://topics.law.cornell.edu/wex/Employment_discrimination (last visited Mar. 17, 2011).
12. *See* FACEBOOK, www.facebook.com (last visited Mar. 17, 2011). These categories on my own Facebook page consist of: sex, birthday, relationship status, interested in (pertaining to sexual orientation), political views and religious views.
13. *Federal Laws Prohibiting Job Discrimination*, EQUAL OPPORTUNITY EMP. COMMISSION, *Discrimination*, http://www.eeoc.gov/facts/qanda.html (last modified Nov. 21, 2009).

makes them to discrimination charges.[14] Therefore, many argue that employers need protection from themselves, and regulation of this practice would rescue them from the temptation to use information found on these sites in the wrong way.[15]

B. Expanding the FCRA—One Solution

Most employers view pre-employment background screening as an essential way to maintain a safe and profitable workplace by protecting an employer from negligent hiring exposure, wrongful termination lawsuits, and incidents of sexual harassment, financial loss, false claims, or theft. This screening often includes obtaining a consumer credit report. The Fair Credit Reporting Act, "FCRA," requires employers to notify and obtain written acknowledgment of that notification from applicants before they are allowed to submit a request for their credit reports.[16] In addition, employers also have to inform applicants of negative information and give them an opportunity to clear up mistakes before employers take any adverse action.[17] In the event employers do take adverse action based on the discovered information, they must also submit formal notification to the applicant that they denied the applicant employment as a result of discovered information.[18]

The purpose of these measures is to protect individuals from adverse action taken against them based on inaccurate or incomplete information in the consumer report file.[19] Ideally, once an applicant is informed that negative information has been found in the consumer report, the applicant will have the opportunity to follow up on these matters with employers before any adverse action is taken.[20] To that end, applicants have some important rights when it comes to the information in their consumer profile. First, while it generally costs a fee to access a consumer report, individuals have a right under the FCRA to access their profile once every twelve

14. Fair Credit Reporting Act, 15 U.S.C. §§ 604(b), 606 (2004).
15. While employers may have reason to fear illegal hiring claims based on use of SNS, they certainly have not shied away from punishing current employees for both improper use of these sites during the work day, as well as information found on employees' networking profile. For an illustrative case on how these issues are treated by the court, see Smyth v. Pillsbury, 914 F.Supp 97 (E.D. Pa. 1996) for when an employee was fired for sending derogatory statements about management via e-mail to coworkers.
16. Fair Credit Reporting Act 15 U.S.C. 604(b), 606.
17. *Id.*
18. *Id*. § 615.
19. Davis, *supra* note 4, at 238-39.
20. Federal Trade Commission, *A Summary of Your Rights under the Fair Credit Reporting Act*, YALE U., http://www.yale.edu/hronline/careers/screening/documents/FairCreditReportingAct.pdf (last accessed Mar. 12, 2010).

months.[21] Second, consumers may dispute incomplete or inaccurate information, and the consumer reporting agency must investigate and remove the information if it is found to be false.[22] Finally, consumers could be entitled to damages in the event a consumer reporting agency, user, or furnisher of a consumer reporting agency violates the FCRA.[23]

The courts have already considered the issue of employers firing or not renewing contracts of employees who violate workplace policies through their web usage,[24] but what about the individuals whose applications are tossed because of information readily available at the click of anyone's mouse? According to one argument, the solution is to amend the FCRA so that "consumer reports" would also include information found on SNSs.[25] This would essentially mean that every time an employer wanted to search the web for a potential applicant, the employer would have to notify that applicant, have the applicant sign a release form, and then notify that applicant in the event the employer discovered negative information on his or her profile page.

Donald Carrington Davis, the advocate of this idea, identifies three serious harms that expanding the FCRA would guard against, including: (1) the danger that employers use inaccurate or irrelevant information to make employment decisions; (2) the lack of accountability which might tempt employers to hire illegally; and (3) the inherent right to privacy violated when employers venture into employees' private lives.[26] To protect applicants and employers from these harms, he proposes broadening the definitions of terms that already exist in the FCRA, including "investigative consumer reports," and "consumer reporting agencies."[27] Davis argues his solution is a "simple" one, stating that "amending these definitions slightly to include social networking services as 'consumer reporting agencies' and making the online profiles that these social networking services store 'investigative consumer reports' simply updates the law to provide continuing protection to candidates and employees as employers find new

---

21. *Id*. Consumers actually have access to *each* credit bureau and select reporting agencies upon written request, which technically could translate into more than one inquiry per year).
22. *Id*.
23. *Id*.
24. *See* Myers v. City of Highland Vill., 269 F. Supp. 2d 850 (E.D. Tex. 2003) (employee fired for making disparaging comments about supervisor on social-networking profile); Malik v. Amini's Billiard & Bar Stools, Inc. 454 F. Supp. 2d 1106 (D. Kan. 2006) (employee terminated for posting resume on internet database). *See also* Snyder v. Millersville Univ., 2008 WL 5093140 (E.D. Pa. 2008) (student teacher fired for posting inappropriate materials on Myspace, and communicating with students inappropriately online).
25. *See generally* Davis, *supra* note 4.
26. *Id*. at 237, 241-48.
27. *Id*. at 251.

ways to investigate their candidates."[28] This overreaching statement takes a leap, essentially equating consumer reporting agencies that furnish credit reports for business purposes to the social networking websites primarily used for recreation.

Of course, while simply amending the definitions to statutes already in place sounds simple enough, the question next addressed by Davis shows the matter to be a bit more complicated. In the ever-expanding world of cyber technology, how does one even begin to discern which social media qualifies as protected by the FCRA? He argues that to distinguish between protected social media and other web material, one must look at the "intent, purpose and expectation" of the service.[29] Where the user intends to publish information for a public purpose, such as in magazines, newspapers, and even blogs, protection is unnecessary because the user has every reason to expect the general public to have access to the information.[30] Conversely, where the user posts information intended for a private community who may view it by invitation only, FCRA protection should be put in place because users would not expect employers to use social media to gain access to their private lives.[31]

This solution is the lone idea and lead contender for reforming employment laws to include internet research as an illegal hiring practice. However, while this solution may be the winner in a one-runner-race, the next section demonstrates that it is far from the flawless remedy its advocates hold it out to be.

III. ANALYSIS

On its surface, Davis' proposal to expand the FCRA to regulate the use of social media in employment decisions is a creative solution to a complex problem. However, despite the solution's apparent simplicity, it is inherently flawed in a number of ways. First, it ignores the real differences between credit reporting agencies and social networking websites. Second, it promotes the viewpoint, perhaps indirectly, that employment is a right rather than a privilege, which is simply not the case; and lastly, it is an unenforceable solution that is likely to produce a false sense of security rather than any real protection for the applicants it aims to guard. This analysis section will deal with each of these issues in turn.

---

28. *Id.*
29. *Id*. at 252.
30. *Id.*
31. *Id.*

A. Social Networking Sites Are Not Like Consumer Reporting Agencies

In arguing the solution to this problem is simply to expand the FCRA to include social networking sites within the definition of "consumer reporting agencies" and "consumer reports," proponents of this legislation assume a large degree of similarity between the two information outlets. This could not be further from the truth, and the differences alone point to the difficulties of lumping these two outlets into the same category, let alone the same definition.

The first and most obvious difference between SNSs and consumer reporting agencies is the party with the ability to control the information contained within the outlet. With a consumer reporting agency, the agency receives the information from various outside sources and organizes and reports it to parties who have the consumer's consent to access the information.[32] While the consumer, whom the information is about, has the ability to view the information and dispute it in the event that it is inaccurate, it generally costs the consumer a fee to check it more than once a year.[33] Importantly, the consumer report contains data that exists regardless of a person's desire to be tracked. Further, the absence of transactions or credit will actually hurt the overall score.[34] Social networking sites, in contrast, are controlled by the user, who has the choice to set privacy settings and may choose not to have an account at all. Consider the following statement made on Twitter's "About Us" segment of their website: "Just remember, how you use Twitter is completely up to you. Follow hundreds of people. Follow a dozen. Post every hour. Post never. Search for your favorite topics and create lists. Or not. You are in control on Twitter."[35] This statement illustrates the very essence of this argument. These social networking sites acknowledge the public's conflicting desires to share information and the need to be able to control the privacy and use of these outlets. Therefore, they are created to be user-friendly so users with all levels of comfort with information sharing are able to participate. Unlike consumer reporting agencies, SNSs represent themselves to users as places where users themselves control their information.

A second difference between these information outlets is the purpose for which they are respectively intended. Consumer reports are a function

---

32. Federal Trade Commission, *A Summary of Your Rights under the Fair Credit Reporting Act*, YALE U., http://www.yale.edu/hronline/careers/screening/documents/FairCreditReportingAct.pdf (last accessed Mar. 12, 2010).

33. *Id.*

34. *Your Credit Score: How it all Adds Up*, PRIVACY RIGHTS CLEARINGHOUSE http://www.privacyrights.org/fs/fs6c-CreditScores.htm#5 (last visited Mar. 17, 2011).

35. *About*, TWITTER, http://twitter.com/about (last visited Mar. 17, 2011).

of the government's need to regulate the banking system.[36] Congress found that the banking system is "dependent on fair and accurate credit reporting and . . . consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit."[37] To this end, consumer reports and the agencies that create them are a mechanism initiated by the government to aid the functioning of the banking system, and other systems that require such information to make essential business decisions.[38] SNSs' purposes, on the other hand, generally range from leisure, to intrapersonal and mass communication, to networking, as the name implies.

To place SNSs within the definition of "Consumer Reporting Agency" and "Consumer Report," is contrary to the plain meanings of the terms and purposes of the statute. Of course individuals are all consumers, but nothing in the mission statement of these social networking sites identifies the purpose of enhancing the accuracy of the banking system, or enabling agencies and businesses to make solid decisions about whether to lend someone money or entrust them with their funds. Consider Facebook's mission statement, for example, which is "to give people the power to share and make the world more open and connected."[39] This intrapersonal focus on connecting the world through sharing hardly aligns with the government's vision for consumer reporting agencies. Myspace too, on its homepage, contends that its focus is to "[drive] social interaction by providing a highly personalized experience around entertainment and connecting people to the music, celebrities, TV, movies, and games that they love."[40] Again, Myspace's obvious social focus does not mirror the straight-lined business focus exhibited by the consumer reporting agency.

Why do these differences matter? They matter because they show that SNS users do not need the same kinds of protection that consumers need from credit bureaus. The definitions themselves indicate how and why the FCRA was created in the first place. It is a targeted collection of laws aimed specifically at protecting consumers who are subject to a practice over which they have relatively little control.[41] Having a consumer report is not something citizens willingly agree to, since most people would prefer to live without the stress of trying to decipher credit reports and the fear that even simple transactions might affect their scores. The need for the FCRA

---

36. 14 U.S.C. § 1681(a)(1) (2006).
37. 14 U.S.C. § 1681 (a)(1)-(3).
38. *See also* 14 U.S.C. § 1681(b). "Other systems" include employers, insurers, agencies entrusted to determine the applicant's eligibility for a government issued license, state or local child support agencies, and those who intend to use the information for a credit transaction, among others. *Id.*
39. Facebook Information, FACEBOOK, http://www.facebook.com/#!/facebook?v=info&ref=pf (last visited Mar. 17, 2011).
40. *Press Room*, MYSPACE, http://www.myspace.com/pressroom (last visited Apr. 11, 2011).
41. 14 U.S.C. §1681 (a)(1-3).

arose partly because the purpose of having consumer reports in the first place is dependent on the report actually being accurate.[42] If there is no public confidence in consumer reports, then they would not be useful, and if there were no way to police these records, then there would be no public confidence in them or acquiescence to their preparation. SNS users, however, can google their own names and check for themselves that their information is accurate. If it is not accurate or does not reflect well on them, they can generally change the information, as Nyugen did to remove his satirical essay. In fact, SNSs are so vastly dissimilar to the consumer reporting agencies regulated by the FCRA, that there is little chance these sites could be effectively regulated by legislation created for an entirely different purpose and for an altogether different group of information outlets. It is a bit like comparing romance novels to law books; at the most fundamental level they are similar in that they both contain words and sentences, but their respective purposes and audiences are so different that they would never appear in the same section of the library, let alone the same shelf. This is one reason why the FCRA will not work to protect applicants against employers using social networking sites. While the legislation itself is easily executed, it will not be as effective against internet searching as it is against consumer reporting agencies.

B. Expanding the FCRA to Include Social Networking Sites Is an Impractical Solution

The previous section argued that the FCRA cannot fully carry out the same objectives for both SNSs and consumer reporting agencies. This section discusses exactly how difficult it would be to regulate employers' use of SNSs simply by expanding the FCRA's definitions of "consumer reporting agencies" and "consumer reports." More specifically, it identifies the difficulties in enforcing such a plan against employers in a way that would not open the floodgates to frivolous litigation.

To illustrate this point, consider what happens when an employer wishes to obtain a consumer report on an applicant. The employer first must obtain the written consent of the subject of the report.[43] Next, it must submit an inquiry to an agency, which, being a capital-driven business, charges a modest fee for its services.[44] Eventually the consumer report is

---

42. Federal Trade Commission, *A Summary of Your Rights under the Fair Credit Reporting Act*, YALE U., http://www.yale.edu/hronline/careers/screening/documents/FairCreditReportingAct.pdf (last visited Apr. 11, 2011).

43. *Id.*

44. Equifax, one of the leading Consumer Reporting Agencies, calls this service "Assessment and Talent Management." *Hiring*, EQUIFAX, http://www.equifax.com/workforce/hiring/en_us (last visited Mar. 17, 2011).

transmitted, and the situation progresses exactly as was detailed in earlier sections. Because the consumer reporting agency is fundamentally a business, it keeps and exchanges records between the agency and the requesting employer, thus leaving a paper trail. When an illegal hiring practices complaint and investigation begins, the consumer has a record of exactly where the employer went to find information, as well as exactly what the report contained.

This is a very neat process for consumer reports, but consider how this same situation would occur if the subject of review were information found on an SNS. The employer could probably obtain consent from the applicant with little problem, but how would it progress from there? Would the consent form specify which Social Networking Sites the employer is allowed to visit, and would it require the employer to keep a record of every site visited in conjunction with the screening process? Without the neutral third party (the equivalent of the consumer reporting agency), there would be no record and no paper trail, and anyone who is minimally technologically savvy could figure out how to erase the computer's history in order to destroy any record of visiting the site. For this reason, it would be nearly impossible to track employers' activity on these sites, and thus nearly impossible to provide an evidentiary basis to validate an illegal hiring claim.

In fact, if the legislature were to expand the FCRA to include social media, then employers would be required to obtain consent from potential hires in order to use these online networking devices. But can the legislature really direct how commercial websites are used and who can use them? Such regulation would restrict the purposes these websites could be used for, with the effect that, although these websites are free and available to all, they could not be used by an employer to learn more information about potential employees. It seems absurd to place this limitation on employers, when one of the major advantages of these information outlets has been to aid in connecting employers to job-seekers. In fact, many employers have done their recruiting via social media such as Facebook and Twitter, and job advertisements appear on the sidebar of personal profiles on a regular basis. Therefore, it would be illogical to let employers *find* potential applicants through SNSs—what has become a major function of social networking devices in general—yet not let employers *find out about* potential applicants through these devices.

Not only would it be practically impossible to police employers when there is no actual record to follow, but even if applicants could prove that potential employers rejected them based on unfavorable information on the internet, applicants would still hardly have a reasonable basis for a lawsuit against an employer when the applicants themselves placed the information on their networking sites. A law that allowed applicants to sue on this basis

would be absurd. If applicants have reason to suspect there is illicit material on their networking page, surely it is their responsibility to remove it, not employers' responsibility to avoid looking at it.

Additionally, expanding the FCRA to cover SNSs is also impractical because, without a neutral third party, there is little formal record of transactions occurring on the internet, and effective regulation under an FCRA-like law would require an altogether separate entity to monitor employers' use of these sites. For credit reports, individuals and businesses alike have to solicit the information they seek directly from the Credit Bureau, because that information is not accessible to individuals as are SNSs. Since users are essentially the ones who produce the information to be reviewed, expanding the FCRA would likely call for Reporting Agencies or the SNSs themselves to prepare reports based on the information found on their SNSs. Therefore, the administrators would ultimately begin serving a commercial function far more complex than simple access to advertising. Without a separate entity to compile information on the internet into a report like that prepared by credit bureaus, employers would look to the network administrators to serve this function. Consequently, the information-sharing aspect of SNSs would morph into an information-selling enterprise which might ultimately discourage the use of these sites.

However, employers would have little incentive to pay an agency or SNS administrator for access to information that is, in general, free to anyone and everyone. Until the information on these networks is only available to employers for a fee, there will not likely be a separate entity tasked with compiling information packages for employers to use in hiring like that produced by credit reporting agencies. Without that third-party intervention, the question then becomes one not of whether the FCRA could effectively regulate this process, but instead whether it is a process worth regulating. Perhaps all of the fears about chilling free speech and opening the avenues for discrimination are just a front for the real culprit of this battle for privacy protection: a generational shift to a sense of entitlement—the viewpoint that employment is more of a right than a privilege.

C. Employment: a Privilege or a Right?

One of the biggest fears of proponents of the plan to expand the FCRA is that the absence of protection for job applicants might "chill" free speech.[45] That is often a legitimate fear where individuals feel they have to restrict what they do or say for fear of adverse action or retaliation by

45. Davis, *supra* note 4.

another party. In this case however, this section asserts that this fear is unfounded and detracts from the real problem that needs to be addressed: illegal employment discrimination.

First, the fact that employers look at social networking websites is not a secret to job applicants, and responsible applicants will act appropriately. Given that anywhere between 60-85 percent of employers are using these methods to screen potential employees, its occurrence should not be a surprise.[46] The reality of the situation is that job-seekers can—and many do—alter their profile pages to present a more professional and appealing image to potential employers.[47]

This is where applicants often diverge into two separate categories: those who see employment as a right for which they should not have to make other lifestyle adjustments, and those who see employment as a privilege they have to earn. Individuals who see employment as a right are the likely group to fear "chilled speech" as the result of online screening. For this group, employment is something an individual is entitled to, and therefore employers have no right to seek beyond the information that they voluntarily and directly present to the employer personally. On the other hand, the opposite group views employment as a privilege to be earned, and therefore respects the fierce competition that occurs within a market economy. This group holds the viewpoint more relevant to job-seeking in the United States. Especially in an economy where there is a shortage of jobs, it is imperative for an individual to put his or her best foot forward. For this reason, closely monitoring every aspect of one's life to appeal best to a potential employer should be regarded as a leg up on the competition who may choose to be less diligent about the information they display to the world via the internet.

If employment is a privilege, then in order to rise above the competition, one must work hard to present a picture to the employer that is

---

46. Amanda Lenhart, *Adults and Social Network Websites*, PEW INTERNET (Jan. 14, 2009), http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites/1-Summary-of-findings.aspx.

47. The only individuals affected by employers' engaging in online screening are those actively applying for jobs, since there are regulations each company has regarding internet usage of employees already in place. Companies that allow their employees access to the internet generally have to abide by an Acceptable Use Policy, or "AUP." One law review article estimated that 77 percent of large American corporations monitor workplace internet usage. Jay P. Kesan, C*yber-working or Cyber-shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 291 (2002). For a closer look at how entities in both the public and private sectors regulate internet usage at work, see *Acceptable Use Policy*, U.S. DEP'T OF THE INTERIOR (May 23, 1997), http://www.doiu.nbc.gov/orientation/acceptable_use.html (a use policy created by the government); *Internet Acceptable Use Policy*, LEE C. (Jan. 2006) http://www.lee.edu/itt/accusepol.asp (a usage policy created by a private university); *IBM Social Computing Guidelines*, IBM, http://www.ibm.com/blogs/zz/en/guidelines.html (last visited Mar. 17, 2011) (AUP created by a private corporation to regulate employees' use of social media).

in line with the ideals and vision of that company.[48] Our society regularly expects people to moderate their speech and personal expression to meet professional standards. Just as job-seekers would not show up to a job interview in the previous night's clothing smelling of cigarette smoke and alcohol, it is equally improper to air one's dirty laundry on the World Wide Web. While it is important to acknowledge that the proponents of this legislation intend to protect only information aimed at private, invitation-only audiences, it is nevertheless naïve of a job-seeker to voluntarily interject information into the stream of communication expecting that it will only reach the specific individuals it was intended for.

It is not a violation of rights if applicants lose job opportunities for placing inappropriate, unprofessional information and images on their networking profiles. These people have the ability to police the web on their own behalf, and therefore there is no need for any law to protect them. Rather, the real problem is when applicants who have clean online profiles face discrimination based on race, age, marital status, sexual orientation, and many of the other personal characteristics easily discoverable on these pages. This is the present danger of using SNSs for hiring purposes: employers may discriminate illegally against applicants. For some applicants, discrimination might be imminent not by cavalier placement of information on the internet, but instead for simply being oneself. A single picture, for instance, reveals at a glance a person's race and gender, and perhaps identifies possible disabilities. For this reason, there is a very real need for some regulation, even if expanding the FCRA is not the panacea for the problem. The next section proposes an avenue down which the legislature might proceed in order to protect individuals from discriminatory hiring practices, not to preserve any non-existent "right" to employment.

IV. SOLUTION

Davis introduces legitimate cause for concern over employers' use of Internet information when hiring.[49] SNSs have created a new way to forge connections, and the reality we face is that privacy lines have blurred

---

48. It is also becoming more common for employers to report discovering the applicant was dishonest on his or her application. One of the newest online business networks, "LinkedIn" actually allows employers to search for employees of applicants' previous places of employment. One executive reported finding references from five of the six employers reported on an applicant's application. These individuals the employer contacted for references were never actually provided by the applicant. *See* Rachael King, *Social Networks: Execs Use Them Too*, BUSINESSWEEK (Sept. 11, 2006), http://www.businessweek.com/technology/content/sep2006/tc20060911_414136.htm.

49. Davis, *supra* note 4, at 237.

considerably. Students have the ability to delve into the lives of their teachers, scholars have the ability to instantly learn information that once would have taken them days or months to discover, and employers now have access to information they would never be permitted to inquire about in an interview. As with the progression of the law in the natural course of history, with these changes, employment law also needs to change. The dangers cautioned by Davis's article should not be ignored, but there is a way to deal with this problem without trying to stretch the solution to another issue to fit the current situation. Instead, new legislation should be enacted to address hiring practices involving SNSs directly. This Comment proposes requiring employers who choose to use the Internet as a screening tool to inform applicants of their intent to do so prior to commencing such screening. This plan is not difficult to implement and serves the purpose of preventing illegal hiring practices by promoting appropriate use of SNSs in hiring, as well as providing a remedy for individuals who suspect discrimination.

Employers often opt for legal safeguards when constructing applications by stating they are "equal opportunity employers," and mentioning they do not discriminate on the basis of race, sex, or religion, among other things. In addition, some employers state that they reserve the right to call the applicant's past employers for references. These safeguards function the same way as a statement notifying applicants that the employer reserves the right to use the Internet as a further character reference. The only major difference is that, should an employer choose to use the Internet as a screening tool, it then becomes mandatory to inform applicants of this fact on the application. This method does not require that applicants divulge any additional information, and they should not be asked to offer screen names, Internet aliases, or a list of networking sites used. Rather, applicants should simply be given fair notice that the employer might conduct an Internet search as part of the hiring process.

Such a method would prove effective for a number of reasons. First, it would put applicants on notice that online appearance will be a significant hiring factor if they are applying for a job in which professional image matters. With so many employers actually using SNSs to promote their businesses, the distinction between private and public lives is far less apparent.[50] At the very least, applicants might be alerted to the fact that this employer believes that one's professional life extends to one's online image. Ultimately, employees who do not share that view are less likely to

50. *See generally* Jake Swearingen, *Social Networking For Business*, BNET (Sept. 5, 2008), http://www.bnet.com/2403-13070_23-219914.html.

thrive at that place of employment and might wish to discontinue their applications as a result.

Second, this method holds employers directly accountable. A mandatory disclosure would likely cause employers to seriously consider whether using SNSs as a screening tool is valuable enough to risk discrimination claims. The result of this might be that fewer employers will use the Internet for screening purposes, but most employers should be able to continue using SNSs and ensure they use it in a non-discriminatory way. For those employers who do choose to use SNSs, they simply must notify applicants that they are doing so. Companies who make themselves vulnerable to discrimination charges are more likely to place limitations on their own hiring managers to avoid any implications of illegal hiring practices. Just as many legal departments advise corporate clients to mention on the application that they are "equal opportunity employers" and to notify applicants of an intention to check resources, they will also likely advise employers to use social networking sites to screen for professional conduct and character alone. Thus, this solution provides the opportunity for employers to first choose whether or not they want to engage in this practice, and second, to self-police the use of these sites or face the possibility of discrimination claims.

Ultimately, when it comes to employers' use of SNSs when hiring, all that applicants are looking for is accountability. The discrimination dangers that seem inherent in Internet use are present because applicants, although aware that many employers use social media, do not know which employers use these methods to screen applicants. The proposed solution eliminates that guesswork, and requires employers to acknowledge the practice and be accountable. Ideally, this would cause employers to think twice about the value of this screening method, and hopefully to employ policies that would protect the company if it chooses to utilize this method. The result of this solution is a regulation which is easier to implement, targeted to the specific problem at hand, and easily supervised by the Equal Employment Opportunity Commission as opposed to the creation of a new agency for this purpose.

V. CONCLUSION

Today, anywhere from a fifth to half of all employers use SNSs to screen applicants. Some are interested in applicants' professional (or unprofessional) conduct, some are interested in their interpersonal communication skills, and some are, well, just interested. With the benefits of employers' ability to verify that the way applicants present themselves to their own networks matches up with the way they presented themselves in an interview or on paper, comes the danger of using that ability for illegal

or improper hiring purposes. Because applicants interject their information into public cyberspace voluntarily on SNSs, these Internet networks might never be completely off-limits to employers. But, because the government has an interest in protecting employees from illegal hiring practices—and in protecting employers from making illegal hiring choices—there must be a law to ensure the appropriate use of SNSs, and a remedy in the event of inappropriate use. While expanding the FRCA would overshoot the needed solution to this problem, the disclosure outlined in the previous section is a simpler and more realistic way to simultaneously protect applicants and provide much needed accountability for employers.