

MYSpace ISN'T YOUR SPACE: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services

*Donald Carrington Davis**

EXECUTIVE SUMMARY

The advent and popularity of online social networking has changed the way Americans socialize. Employers have begun to tap into these online communities as a simple and inexpensive way to perform background checks on candidates. However, a number of problems arise when employers base adverse employment decisions upon information obtained through these online searches. Three basic problems or issues accompany searches of online profiles for employment decisions: (1) inaccurate, irrelevant, or false information leads to unfair employment decisions; (2) lack of accountability and disclosure tempts employers to make illegal employment decisions; and (3) employer searches of an employee's online social life violate an employee's legitimate expectation of privacy.

Because searches of online social networking services, such as "MySpace" and "The Facebook," only stand to become more prevalent among employers, the law must expand to ensure adequate protection to users of these websites from unfair, illegal or arbitrary employment decisions. Employers also stand to gain from such an expansion of legal protections because they will be accountable to make good employment decisions. The original purposes of the Fair Credit Report Act ("FCRA") permit—and demand—its expansion to cover the potential problems for candidates and employees caused when employers search for a candidate or employee's online social networking profiles. This

* Don expects his Juris Doctor degree from The Ohio State University Moritz College of Law, Columbus, Ohio, in May 2007. He received his Bachelor of Arts in Political Science from North Carolina State

solution effectively strikes an agreeable balance between an employer's right to know about candidates for employment and its employees and an employee's or candidate's right to privacy and fair employment decision making.

I. INTRODUCTION AND BACKGROUND

Online social networking services, which include such popular online communities as MySpace¹, The Facebook², and Friendster,³ have begun to dominate and define the way many people socialize, especially teenagers and young adults. MySpace allows its members to create profiles with personal information, communicate with others in their online network, and enjoy a variety of other membership benefits, including listening to music made available by many musical artists who maintain profiles on MySpace. MySpace expresses a purpose to host private social communities through its service.⁴ The Facebook began as a social networking website for college students, but it has since expanded to provide networks for high school students, professionals, and alumni; it now allows almost anyone to create a profile. Numerous other social networking websites focus on establishing networks for everything from activism to particular professional affinities. These websites provide users with avenues and outlets to express themselves freely, meet other people, and keep in touch with the people they know.⁵

University, Raleigh, North Carolina, in December 2002. Don would like to thank Professor Peter Swire and Guillermo Gabriel Zorogastua for the insight and contributions they have provided.

¹ MySpace Home Page, <http://www.myspace.com> (last visited Dec. 12, 2006).

² Facebook Home Page, <http://www.facebook.com> (last visited Dec. 12, 2006).

³ Friendster Home Page, <http://www.friendster.com> (last visited Dec. 12, 2006).

⁴ "Create a private community on MySpace and you can share photos, journals and interests with your growing network of mutual friends!" MYSPACE, ABOUT US, <http://www.myspace.com/Modules/Common/Pages/AboutUs.aspx> (last visited Dec. 18, 2006).

⁵ One popular online encyclopedia estimates that over 200 social networking websites exist. *See* WIKIPEDIA, SOCIAL NETWORK, http://en.wikipedia.org/wiki/Social_Network (last visited Nov. 26, 2006).

With over one hundred million accounts worldwide⁶ and fifty-six million unique users in the United States,⁷ MySpace currently stands as the leader in online social networking, and it continues to grow at a pace of approximately 230,000 new profiles a day⁸. This very popular site commands the loyalty of nearly eighty percent of visitors to online social networks.⁹ The Facebook currently holds first place in the online world as both a college-based social network¹⁰ and for the uploading and storage of photographs.¹¹

While many over the age of thirty have begun rushing to become part of the online social networking world, the largest and most significant group of online social network users comes from the generation commonly known as Generation Y, young adults now in their late teens to twenties.¹² Unlike the much older adults who shaped, wrote, and interpreted the privacy laws applicable today, these young adults grew up in an age of vast technological expansion that has fostered a world of instantaneous communication and with it the need for new modes of thinking in the area of privacy. As these young adults enter the workforce, they face a realm of unfamiliar thinking about the meaning of digital privacy.

⁶ MySpace's 100 millionth account was created August 9, 2006. See Rupert Murdoch, *Rupert Murdoch Comments on Fox Interactive's Growth*, SEEKING ALPHA, Aug. 9, 2006, <http://internet.seekingalpha.com/article/15237>.

⁷ Although MySpace has over 100 million accounts, this does not accurately reflect how many distinct individuals use social networking services, as some users create more than one account. See Anick Jesdanun, *Youths No Longer Predominant at MySpace*, ASSOCIATED PRESS, Oct. 5, 2006, available at <http://abcnews.go.com/Technology/wireStory?id=2534413>.

⁸ Patricia Sellers, *MySpace Cowboys*, FORTUNE, Aug. 24, 2006, available at http://money.cnn.com/magazines/fortune/fortune_archive/2006/09/04/8384727/index.htm.

⁹ Reuters, *MySpace gains top ranking of US Web sites*, USA TODAY, July 11, 2006, available at http://www.usatoday.com/tech/news/2006-07-11-myspace-tops_x.htm.

¹⁰ Susan Kinzie & Yucki Noguchi, *In Online Social Club, Sharing Is the Point Until It Goes Too Far*, WASHINGTON POST (Sep. 7, 2006), available at http://www.washingtonpost.com/wp-dyn/content/article/2006/09/06/AR2006090601805.html?nav=rss_education.

¹¹ FACEBOOK, INSIDE FACEBOOK ENGINEERING, http://www.facebook.com/jobs_engineering.php (last visited Dec. 15, 2006).

¹² Jesdanun, *supra* note 7.

Surveys differ on how many employers include some form of internet search of candidates in their applicant screening process, but all agree that it has become an increasingly popular trend among employers.¹³ One survey found that sixty-three percent of employers that search social networking profiles online have rejected candidates based upon information found within those profiles.¹⁴ Many employers consider searching a candidate's MySpace or Facebook profile an inexpensive and convenient peek into the candidate's life and character.¹⁵ Until recently, when news articles and "blog" entries began to appear on this topic and career placement professionals began to warn students of the risks of posting information about themselves in their social networking websites, online social networking users remained generally unaware of the fact that many employers were rejecting them because of something the employer found on their MySpace profile.¹⁶

Modern young adults demonstrate a willingness to post information about themselves on these websites because of their conception of privacy in today's world. Americans know that a wealth of information about them floats around in the electronic world—outside the realm of their physical control—yet, Americans do not necessarily consent to sharing that information with parties that have no proper or relevant use for it. Congress has enacted laws to help to ensure that only appropriate individuals and entities

¹³ Alan Finder, *For Some, Online Persona Undermines a Résumé*, N.Y. TIMES, June 11, 2006, available at <http://www.nytimes.com/2006/06/11/us/11recruit.html>.

¹⁴ Press Release, CareerBuilder.com, 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 (Oct. 26, 2006), available at http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr331&sd=10%2f26%2f2006&ed=12%2f31%2f2006&siteid=cbpr331&sc_cmp1=cb_pr331_ (on file with author).

¹⁵ See Alison Doyle, *MySpace, Facebook and More*, ABOUT: JOB SEARCHING, available at <http://jobsearch.about.com/b/a/217342.htm> (last visited Dec. 15, 2006) ("Employers have been known to peruse MySpace and Facebook, along with blogs and websites of prospective employees.").

may access some of one's personal information that lies beyond her physical control and that the information about an individual portrays her accurately and fairly. Specifically, Congress communicated, through the Fair Credit Reporting Act (FCRA),¹⁷ its intent to ensure that an individual's eligibility for employment is based on a consumer report free from inaccurate or irrelevant information.¹⁸

Members of Generation Y do not consider their online profiles the province of their employer much in the same way an older generation would think it improper and invasive for an employer to show up at an employee's private party unannounced. The existence of the internet undoubtedly has changed the way present society interacts. While members of this generation reasonably understand that many people may easily access information about them posted on the internet, they believe that what they do in their private social lives is none of their employer's business. As long as their activity does not violate the law, does not negatively impact business or job performance, and does not expose their employer to liability, it should not become the basis for adverse employment decisions. While employers have the right to know who their applicants and employees are, they must keep in mind the important separation between the professional and private lives of their candidates and employees. Making assumptions about a person's professionalism based upon information obtained out of context on a website

¹⁶ One recent college graduate reported that once he removed a satirical essay he published on a social networking site for students, he began to receive invitations to interview and has since received several job offers. Finder, *supra* note 13.

¹⁷ 15 U.S.C. § 1681 *et. seq.* (2000).

¹⁸ *See* Rasor v. Retail Credit Co., 554 P.2d 1041, 1045 (Wash. 1976) ("The Fair Credit Reporting Act was adopted 'to protect an individual from inaccurate or arbitrary information about himself in a consumer report that is being used as a factor in determining the individual's eligibility for credit, insurance or employment.'" (quoting Porter v. Talbot Perkins Children's Servs., 355 F. Supp. 174, 176 (S.D.N.Y. 1973))), *and* Rasor, 554 P.2d at 1045 ("The general purpose of the FCRA is to protect the reputation of a consumer, for once false rumors are circulated there is not complete vindication." (quoting Ackerley v. Credit Bureau of Sheridan, Inc., 385 F. Supp. 658, 659 (D. Wyo. 1974))).

designed solely for social purposes violates a basic tenet of conventional wisdom—you cannot always believe what you see.¹⁹

Lawmakers and policymakers must begin to reconsider the traditional physical conceptions of privacy (i.e., thinking about privacy within physical boundaries, such as a home or an automobile) in order to meet the demands of the members of this new tech-savvy generation that have proven much more apt to share and communicate in the world wide web than their ancestors. In a world where maintaining absolute discretion in every aspect of one's life seems both impossible and impractical, Congress must begin to respond by adopting reasonable privacy protection measures. These measures should conform to the modern concept of an employee's expectation of privacy—an expectation that is as strong as ever—but now with virtual boundaries rather than purely physical ones.

The scope of this article is limited to private employers who are subject to relevant provisions of federal employment-related laws. It examines the problems that might arise when employers use online social networking profiles to make employment decisions and proposes a solution that balances an employee's reasonable expectation of privacy and an employer's rights to make informed employment decisions. Part II examines the problems that accompany an employer's search of social networking profiles. Part III examines and analyzes the federal law in place that is designed to protect employee privacy rights with regard to background checks, it and discusses the

¹⁹ Employment lawyer George Lenard asserts that employers must not forget that the lessons of conventional wisdom that applied to earlier modes of communication, such as newspapers and television, also apply to the Internet. George Lenard, *More on Facebook et al. in Recruiting and Hiring*, George's Employment Blawg, <http://www.employmentblawg.com/2006/more-on-using-facebook-et-al-in-recruiting-and-hiring/> (last visited Apr. 14, 2006). An old adage, "Not everything you hear/read is true," easily evolves into "Not everything you see/read on the Internet is true." *Id.* Applied to candidates for employment, "Not everything you see on MySpace is true or accurate." *Id.*

policy that breathes life into this law. Finally, Part IV proposes an expansion of the FCRA that will balance the employee's expectation of privacy and right to know, as a consumer, what information exists about her, with an employer's right to know its applicants and employees. With a simple definitional expansion, the FCRA would easily extend its protections to those who have used, use, and will use online social networking as a part of their off-duty lives without unduly burdening employers.

II. SPECIAL PROBLEMS CREATED BY EMPLOYER SEARCHES OF ONLINE SOCIAL NETWORKING SERVICES

When employers use online social networking profiles to make decisions about hiring, retention, and promotion, they risk creating a number of problems for themselves and their candidates and employees. Currently, employers may search these online profiles without ever disclosing the search, the results of the search, or the reason for any attendant adverse decision regarding the candidate or employee. The doctrine of employment-at-will guarantees this unfair result despite many attempts to modify the doctrine to avoid and mitigate such results. Federal and state exceptions to the doctrine exist to protect employees from unfair and arbitrary decisions, and logically they should extend to protect against unfair decisions based upon an individual's online persona.

First, Congress had reason to enact the FCRA, in part, because it perceived that inaccurate and even completely fabricated information about individuals is legion. Decisions based upon inaccurate information unfairly impact the reputation, credit-worthiness, and well-being of individual candidates and employees and should be made known to the individual to allow for prompt and timely correction. Second, undisclosed online searches of candidates and employees provide information that can tempt an ill-

meaning employer to violate laws—laws that are easy to violate without a system of information accountability in place. Third, employees’ and candidates’ expectations of privacy in their personal, off-duty lives give them respite from the always-scrutinizing eye of their employer. If privacy is to retain any value in a world where people can no longer hide their lives behind physical boundaries, the law must require employers to provide notification of, obtain authorization for, and disclose the results of online social networking searches of candidates and employees.

A. False, Inaccurate and Irrelevant Information that Results in Unfair Adverse Employment Decisions

One of the most prominent and legitimate concerns of employee privacy advocates is in the problem of inaccurate or false information, especially that which lies beyond an individual’s ability to control. Employers risk making poor employment decisions based upon information that may paint an inaccurate or unfair portrait of the candidate or employee. Varying degrees of problems based upon inaccuracy exist, from fake profiles created about a person²⁰ by another, to inaccurate assumptions formed on information that may be true, but not representative, of a person’s background or character. When an employer bases an adverse decision upon bad or incomplete information, it violates the very public policy to protect employees that brought about actions by the Congress and state legislatures.

Many have heard the almost trite admonishment not to believe everything one sees and hears. A single photograph of someone does not accurately portray what she

²⁰ Ryan Walker, a Chicago resident, realized he had fallen victim to “profile poaching” on MySpace when someone approached him at a local bar and asked if his name was ‘Justin.’ The profile poacher had taken Mr. Walker’s photographs from his MySpace page and uploaded them to a fake MySpace profile. Cheryl

looks like as a whole person; moreover, it certainly does not portray the totality of her character. However, one photograph placed on a MySpace profile can eliminate an applicant from consideration for employment if the employer makes assumptions about the person based upon what an agent of that employer saw in the photograph. One's personal values and bias, which vary from one recruiter or human resources director to another, can form the basis for abuse, unfairness, and worst, adverse employment decisions in this area. Applicants, employees, and employers all suffer.

One troubling example of a tactic that the law, in its current state, may promote is malicious manipulation of online social network profile information between competitors for employment. A candidate competing for a highly coveted job, for which she believes the employer may run an online search of the candidates, may create a false profile for her competitor with false and damaging information. Her competitor does not know that this profile exists—and may never find out—since the employer is not required to tell her that it decided not to choose her based upon the profile that it found about “her.” The maliciously manipulative candidate for the job might get the position even if the aggrieved candidate was better qualified for the job. While this may seem like an extreme hypothetical, it is one that is nonetheless possible under the legal status quo, and the competitive nature of the employment market provides an incentive to take advantage of this weak point in the law.

To a lesser degree, and absent malicious intent, problems arise when employers find information about a candidate through someone else's profile. Even when an individual maximizes her expectation of privacy by opting for the most protective privacy

Burton, *Profile Poachers*, ABC7, Nov. 13, 2006, http://abclocal.go.com/wls/story?section=special_coverage&id=4758493.

settings provided by a social networking service, such as hiding personal information from non-network users, she may still fall victim to having information posted about her that she did not consent to having posted and that she may be unaware even exists. While she has done everything possible to prevent an employer from reaching into her off-duty personal life, she still cannot “hide.”

Situations such as these call for new measures of fairness in employer searches of online profiles, measures that give the candidate or employee a way both to know that the information about them exists and to ensure its accuracy, relevancy, and truth, or to have it removed.

Other harms result when employers make incorrect assumptions based upon information posted on an actual profile. Often, online social networking users post photographs taken at social events of themselves and others on their online profiles. To them, it is an excellent and efficient way to share these photographs with many people in their online social network at once. However, if an employer sees photos of a candidate or employee at parties, the employer may unfairly and incorrectly conclude that Jane Doe is a partier or an alcoholic. An agent of an employer may tend to forget her own youthful indiscretions and quickly pass judgment on the character of an applicant or employee based upon an incomplete and inadequate portrait of that person. People create their online social networking profiles with a limited social purpose in mind. If these profiles were meant to portray the person as a whole to be used in determining a person’s worthiness for employment, Jane Doe would build a profile that more accurately portrays who she is as a whole person, not just who she is outside of work when her professionalism is not at issue.

B. A Back Door to Unlawful Employment Discrimination

Employers, currently not required to disclose their searches of candidate and employee profiles, may easily fall into temptation to eliminate candidates from consideration to whom they would not otherwise be able to deny employment opportunities. Congress enacted Title VII of the Civil Rights Act of 1964²¹, the Age Discrimination in Employment Act²², and the Americans with Disabilities Act²³, in part, to eliminate discrimination in employment based on immutable characteristics. Title VII, for example, makes it unlawful for an employer “to fail or refuse to hire or to discharge any individual, or otherwise discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual’s race, color, religion, sex, or national origin.”²⁴ As a result, when hiring employees, employers may not properly ask questions pertaining to some of these protected categories unless they are relevant to a bona fide occupational qualification²⁵.

Online social networking profiles often present personal information that would not be properly the subject of employer–employee dialogue within the scope of an employment decision process. For example, an employer may not be able to ask John Doe what religion he practices during his interview or even after he has begun employment. Any adverse decision based upon John’s religion (or non-religion) that an employer makes subsequent to discovering, by John’s own admission, that he is a

²¹ 42 U.S.C. § 2000a, et seq.

²² 29 U.S.C. § 621, et seq.

²³ 42 U.S.C. § 12101, et seq.

²⁴ 42 U.S.C. § 2000e-2(a)(1) (2000).

²⁵ A bona fide occupational qualification is a minimum qualification requirement that is a prerequisite to the performance of a particular job. This limited exception to Title VII permits an employer to hire employees based on their religion, gender, or national origin if those factors are “reasonably necessary to the normal operation of that particular business or enterprise.” For example, an employer may hire a female to model feminine apparel or a male to model male apparel. 42 U.S.C. § 2000e-1 (2000).

member of a particular church or faith, would be impermissible yet obvious enough to make the illegal decision actionable under the civil remedy provision of Title VII²⁶. However, if his employer were to discover this fact through a covert search of his MySpace profile, without his knowledge, the employer could take adverse action against him without his ever knowing why, leaving him with little or no remedy against his employer for its illegal adverse decision.

In a similar hypothetical, John Doe's best friend suffers from advanced HIV and John regularly gives money and participates in fundraisers to benefit HIV/AIDS research. John's profile reflects his unusually strong and active support for HIV/AIDS-related initiatives. Upon viewing his profile as a part of its "background check" of John, the human resources director assumes that John is HIV-positive and fears that hiring him would drive up the company's health insurance costs, and, as a result, he sends John a standard rejection letter. The employer's decision, probably a violation of the Americans with Disabilities Act²⁷, seems innocuous to John. Little does he know that his benevolence and proud public support for these causes precluded him from getting the job that he had always wanted.

Should John have known better than to show his support for a valid, if not worthy, but no less legal cause? Or should the employer have known better than to make assumptions about John based on an incomplete picture of who he is as a person and a

²⁶ 42 U.S.C. § 2000e-2(a)(1).

²⁷ The Americans with Disabilities Act makes it unlawful to deny a person employment or public accommodations based on a real or perceived disability. 42 U.S.C. §12112(a) (2000). If John is not actually HIV-positive, but his employer or potential employer regards him as such and consequently denies him employment, his employer has violated the ADA. 42 U.S.C. § 12102(2)(C) (2000). The Supreme Court explained Congress' policy reasoning in making the "regarded as disabled" theory available in legislation that preceded but inspired the ADA: "Congress acknowledged that society's accumulated myths and fears about disability and disease are as handicapping as are the physical limitations that flow from actual impairment." *Sch. Bd. of Nassau County v. Arline*, 480 U.S. 273, 284 (1987).

professional, and to then discriminate against him in violation of federal law? In this case, the employer declined to hire John because of an unfounded fear and baseless presumption. The burden must fall on the employer to assemble a fair and accurate portrait of its employees and candidates for employment based upon complete and verifiable information, especially when the candidate or employee has every right to express himself freely through his online persona. The law must ensure that John knows precisely why his would-be employer did not select him so that he will have a fair chance to provide correct and accurate information and exercise his legal remedies if he is denied employment wrongfully thereafter. Had the employer been required to disclose its search of John's MySpace profile, it might have been deterred from its decision not to hire him, knowing that its reasons for that decision might become obvious to John. While an employer may view the solution proposed in Part IV of this note as too restrictive, it will help reduce employer liability for discriminatory employment decisions that would violate federal law by creating accountability and removing the temptation to take adverse action for illegal reasons.

C. Expectation of Privacy in Off-Duty Conduct

On its face, to many this may seem an issue of naïve youth stupidly posting personal information publicly for the whole world to see. Ostensibly, by making information available that they know—or should know—that almost anyone can see, they have lost their expectation of privacy and thus the issue is moot. In the view of some, they have assumed the risk that their parents, potential employers, or anyone else might be able to find out what they do on a Saturday night or a Sunday morning. However, some evidence suggests the opposite: Americans *do* expect privacy in their non-working

lives. While information on these online profiles may be seen by many, including people who are not a member of an individual's online social network, it takes a search to produce the profile and the information. When a candidate for employment applies for a position, she does not e-mail her potential employer the URL for her MySpace profile and invite her employer to view its contents; an employer must use search methods to find the information just as it must make an affirmative request for a candidate's consumer report. The latter search currently falls within the ambit of reasonable privacy protection for the employee; the former search, despite being accompanied by an even greater risk of false or irrelevant information, does not.

A number of lifestyle protection laws enacted by states, along with some specific federal laws and the common law of privacy, suggest that when Americans leave work, they expect to be let alone²⁸. These laws prevent employers from snooping too far into the personal lives of employees, especially when what they would find has no bearing on their business interests or the employee's job performance. States that have enacted such lifestyle laws have begun to erode the employment-at-will doctrine and have firmly codified an expectation of privacy in employees' off-duty lives when their off-duty conduct has no bearing on the employer's business interests. Colorado and North Dakota have both enacted sweeping statutes that forbid discrimination in employment decisions on the basis of off-duty behavior.²⁹ Both statutes provide exceptions when an employee's off-duty behavior conflicts with a bona fide occupational requirement, an employee's job

²⁸ For a more in-depth discussion of the provisions of these state laws, see Pagnattaro, *infra* note 35, at 640.

²⁹ COLO. REV. STAT. 24-34-402.5 (2006) (forbids termination by employer based on *any* lawful activity conducted off the premises of the employer during non-working hours) (emphasis added); N.D. CENT. CODE §14-02.4-03 (2004) (forbids failing or refusing to hire in addition to forbidding discharge based on lawful off-duty conduct during non-working hours).

responsibilities, or an employer's essential business interests.³⁰ California's legislature, which has enacted the broadest and most employee-friendly of these statutes, did not include similar language that would accommodate an employer's business necessity or conflicts of interest in basing adverse employment decisions on off-duty conduct.³¹ New York's legislature enacted a statute that establishes four categories upon which employers may not base employment decisions: legal recreational activities, consumption of legal products, political activities, and union membership³². Other states have enacted much more limited statutes protecting specific categories of lawful off-duty conduct and lifestyle, including consumption of tobacco products, sexual orientation, and marital status. In a world where people simply have begun to conduct much of their social lives over the internet, the same expectations apply: an employer should not be snooping into an employee's personal life when it has nothing to do with business.

Many have written in the area of employee privacy law, mostly regarding an employee's right to privacy within the scope of her employment. Recently, law reviews and journals have begun to entertain more scholarship discussing an employee's off-duty privacy. While the views and proposals represent varying degrees of employee protection, most seem to agree that employees enjoy the highest expectation of privacy with regard to their employer when they are away from work when their off-duty conduct does not significantly impact their employer's business or subject their employer to liability.³³

³⁰ COLO. REV. STAT. §24-34-402.5(1)(a),(b) (2006); N.D. CENT. CODE §14-02.4-03 (2004).

³¹ CAL. LAB. CODE §98.6(a) (West 2003) ("No person shall discharge an employee or in any manner discriminate against any employee or applicant for employment because the employee or applicant engaged in any conduct . . . described in subdivision (k) of Section 96.").

³² N.Y. LAB. LAW 201-d (McKinney 2006).

³³ See Terry Morehead Dworkin, *It's My Life—Leave Me Alone: Off the Job Employee Associational Privacy Rights*, 35 AM. BUS. L.J. 47, 94, 95 (1997).

Some scholars have noted that Americans' conceptualization of privacy rests upon the idea of protection of personal autonomy.³⁴ Professor Stephen D. Sugarman describes this as "the importance we place on giving people the liberty to shape and act out their own lives as they wish, free from the scrutiny of how others might think about that conduct or what they might say about it."³⁵ Professor Terry Dworkin explains that part of the importance that privacy plays in our society rests upon the fact that privacy encompasses a right to self-determination and "to define who we are."³⁶ Self-determination includes the freedom to associate with the people one chooses.³⁷

If these statements accurately reflect how Americans feel about privacy, American employees should have the ability to expect privacy in all aspects of their personal lives, whether conducted within the online community or within the physical confines of their homes or social establishments. Employers might easily be able to discover what their employees are doing outside of the workplace, but thinking about employee privacy in terms of Professors Sugarman's or Dworkin's definitions means shaping and acting out one's personal life without having to worry about the consequences of what one's employer thinks or says about that lawful conduct. Privacy seems more about autonomy and the right to define oneself free from the consequences of others' judgment than about some physical notion of hiding from those who might be watching.

³⁴ Catherine L. Fisk, *Privacy, Power and Humiliation at Work: Re-Examining Appearance Regulation as an Invasion of Privacy*, 66 LA. L. REV. 1111 (2006).

³⁵ Stephen D. Sugarman, "Lifestyle" Discrimination in Employment, 24 BERKELEY J. EMP. & LAB. L. 377, 403 (2003).

³⁶ Dworkin, *supra* note 29, at 94-95.

³⁷ *Id.*

Several privacy advocates have called for severely limiting the use of off-duty conduct in making employment decisions. These authors' solutions range from suggestions that employers be more mindful of privacy rights³⁸ to proposing federal "lifestyle discrimination" legislation designed to limit greatly the ability of an employer to make an adverse employment decision based upon off-duty conduct.³⁹ "Arguably, as long as [employees] are fulfilling their job responsibilities, they are off their employer's moral, social and political clock."⁴⁰

One case in Illinois, *Johnson v. K-Mart*, demonstrates the important expectation of privacy that employees have during their off-duty private lives. Fifty-five plaintiffs brought an action for invasion of privacy based upon unauthorized intrusion into their seclusion.⁴¹ K-Mart hired private investigators to pose as employees in one of its distribution centers in Illinois and to record employees' conversations and activities both at work and at social gatherings outside of work, which they then released to K-Mart.⁴² K-Mart admitted that it had "no business purpose for gathering information about employees' personal lives."⁴³ The plaintiffs maintained a reasonable expectation of privacy in their conversations with coworkers, especially during social gatherings outside of work. They did not expect their employer would use covert and deceptive methods to

³⁸ See, e.g., Dworkin, *supra* note 29.

³⁹ See, e.g., Ann L. Rives, Note, *You're Not the Boss of Me: A Call for Federal Lifestyle Discrimination Legislation*, 74 GEO. WASH. L. REV. 553 (2006); see also Marisa Anne Pagnattaro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct As the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L. 625 (2004).

⁴⁰ Pagnattaro, *supra* note 35, at 627.

⁴¹ *Johnson v. K Mart Corp.*, 723 N.E.2d 19992, 1196 (Ill. App. 2000).

⁴² *Id.* The reports contained information about the employees' family matters, sex lives, and other personal and private matters such as health problems. This is the kind of information that is very similar to what an employer can find by investigating an employee's social networking profile. In both cases, the employee is unaware of the intrusion.

⁴³ *Id.* at 1197.

peer into their private social lives.⁴⁴ The court found that “a material issue of fact exist[ed] regarding whether a reasonable person would have found [K-Mart’s] actions to be an . . . objectionable intrusion.”⁴⁵

In much the same way, employees today who use social networking as a way to communicate among peers outside the scope of their employment reasonably do not expect their employer to pry into their private lives by sending agents into their online social gatherings. K-Mart spied on its employees by sending its covert agents into private social gatherings to obtain information about its employees, assumedly with the purpose of evaluating their fitness for continued employment. We now see employers secretly sending their agents into the online social gatherings of their employees. While the physical boundaries have disappeared, employees’ reasonable expectations have not.

III. THE FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act, enacted in 1970 and given effect in 1971, served as Congress’ response to a then-growing problem in the United States of inaccurate credit reports that caused a variety of harms to consumers. One such class of consumers Congress specifically and explicitly intended to protect is employees whose employers perform background checks on them as both a pre-condition to employment and an ongoing method of “keeping tabs” on them. Before this Act, little or no protection existed for a candidate for employment who was denied employment or an employee who was fired because of false or inaccurate information on the consumer report that her employer obtained from a private consumer reporting agency. She had no right to know

⁴⁴ *Id.* at 1196.

⁴⁵ *Id.* at 1197.

that she was the subject of a credit check and no right to know that she was denied employment, fired, or demoted based on information on her consumer credit report.

Inaccurate, incomplete, irrelevant, or false information could easily form the basis for very unfair employment decisions. In fact, abuse within the credit reporting industry was so rampant that many credit reporting agencies required investigators to fill quotas of negative information on consumers.⁴⁶ To do this, investigators often made up false information and submitted that information to the credit reporting agency.⁴⁷ The credit reporting agencies often included in their reports lifestyle information collected by investigators, leading, inevitably, to a consumer being denied employment based upon a credit report that was, if only in part, untrue and one that certainly contained irrelevant or incomplete information.⁴⁸

When it enacted the FCRA, Congress stated its underlying purpose, policy, and intent to ensure that decisions affecting extension of credit, insurance, and employment, among other things, are based upon fair, accurate, and relevant information about consumers.⁴⁹ Federal appeals courts have held that the Fair Credit Reporting Act must be construed liberally in favor of the consumer.⁵⁰ Clearly, Congress enacted the FCRA to protect the employee from the far-reaching arm of the employer with respect to an employer's inquiry into the private lifestyle matters of the employee.

⁴⁶ ELECTRONIC PRIVACY INFORMATION CENTER, THE FAIR CREDIT REPORTING ACT AND THE PRIVACY OF YOUR CREDIT REPORT, <http://www.epic.org/privacy/fcra/> (last visited Dec. 20, 2006).

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ 15 U.S.C. §1681(b) (2000); *see also* Jones v. Federated Fin. Reserve Corp., 144 F.3d 961 (6th Cir. 1998); Guimond v. Trans Union Credit Info. Co., 45 F.3d 1329 (9th Cir. 1995); Ackerley v. Credit Bureau of Sheridan, Inc., 385 F. Supp. 658 (D. Wyo. 1974); Retail Credit Co. v. United Family Life Insurance Co., 203 S.E.2d 760 (Ga. App. 1974); Rasor v. Retail Credit Co., 554 P.2d 1041 (Wash. 1976).

⁵⁰ *Jones*, 144 F.3d at 964; *Guimond*, 45 F.3d at 1333.

The FCRA allows employers to obtain a “consumer report” from a “consumer reporting agency” for the purpose of making any significant employment decision from hiring to termination.⁵¹ Congress defined a “consumer report” as information (oral, written, or other communication) provided by a “consumer reporting agency” about credit matters as well as about a person’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.”⁵²

Another kind of “consumer report,” called an “investigative consumer report,” contains information obtained through personal interviews with friends, neighbors, and associates of the consumer on a consumer’s character, general reputation, personal characteristics, or mode of living.⁵³

Either a “consumer report” or the more subjective “investigative consumer report” must be obtained through a “consumer reporting agency,” defined as “any person who 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.”⁵⁴

The FCRA requires three essential mechanisms for due process to ensure the accountability of employers who procure and use background information of its employees: notice, authorization, and disclosure. When an employer seeks to obtain any consumer report for employment purposes, the employer must provide the employee with

⁵¹ Fair Credit Reporting Act [hereinafter FCRA] §604(a)(3)(B), 1681b(a)(3)(B) (2000).

⁵² FCRA § 603(d)(1), 15 U.S.C. § 1681a(d)(1).

⁵³ FCRA § 603(e), 15 U.S.C. § 1681a(e).

⁵⁴ FCRA § 603(f), 15 U.S.C. § 1681a(f).

certain notices and certifications⁵⁵. First, an employer must provide the employee or applicant written notice that the employer intends to obtain a consumer report for employment purposes.⁵⁶ As part of the first step, the employer must obtain the employee's or applicant's written authorization to obtain her consumer report.⁵⁷ Before receiving the consumer report, the employer must certify to the consumer reporting agency that it has complied with these notice requirements⁵⁸ and that the information in the consumer report will not be used in violation of any applicable federal or state law or regulation regarding employment opportunity.⁵⁹

Before taking any adverse action based upon information contained in the consumer report, the employer must provide the applicant or employee with a copy of both the consumer report upon which it would base its decision⁶⁰ and a copy of the Federal Trade Commission's publication, "A Summary of Your Rights Under the Fair Credit Reporting Act."⁶¹

If the employer plans to procure an "investigative consumer report," the FCRA requires that it make additional disclosures to the consumer⁶³: No later than three days after requesting a report, the employer must provide the applicant or employee with written disclosure that it may obtain an investigative consumer report.⁶⁴ This disclosure must inform the applicant or employee of her right to request additional information about the nature or scope of the background investigation and must include the FTC's

⁵⁵ FCRA § 604(b), 15 U.S.C. § 1681b(b).

⁵⁶ FCRA § 604(b)(2)(A)(i), 15 U.S.C. § 1681b(b)(2)(A)(i).

⁵⁷ FCRA § 603(o)(2)(A)(ii), 15 U.S.C. § 1681b(b)(2)(A)(ii).

⁵⁸ FCRA § 604(b)(1)(A)(i), 15 U.S.C. § 1681b(b)(1)(A)(i).

⁵⁹ FCRA § 604(b)(1)(A)(ii), 15 U.S.C. § 1681b(b)(1)(A)(ii).

⁶⁰ FCRA § 604(b)(3)(A)(i), 15 U.S.C. § 1681b(b)(3)(A)(i).

⁶¹ FCRA § 604(b)(1)(A)(ii), 15 U.S.C. § 1681b(b)(1)(A)(ii).

⁶³ FCRA § 606(a), 15 U.S.C. § 1681d(a).

⁶⁴ FCRA § 606(a)(1)(A), 15 U.S.C. § 1681d(a)(1)(A)..

summary of rights.⁶⁵ The employer must then certify to the consumer reporting agency that the employer has and will comply with all notice and disclosure requirements.⁶⁶ Finally, upon written request made by the applicant or employee within a “reasonable time,” the employer must provide complete written disclosure of the nature and scope of the investigation that it requested.⁶⁷

The FCRA provides civil remedies for those injured by an employer’s failure to comply with the provisions mentioned above.⁶⁸ An employer or agent of such an employer who knowingly or willfully procures a consumer report under false pretenses may also be liable criminally and could face fines and incarceration of up to two years.⁶⁹

IV. EXPANDING THE FCRA TO REACH ONLINE SOCIAL NETWORKING SERVICES

The law should empower employers to research their candidates carefully, and employers should do so by taking advantage of modern methods, such as online searches. The law should also alleviate employees of fears that their employers may lurk, unbeknownst to them, in the shadows of their online personas. The law must continue to regard fairness, accuracy, and relevancy as primary values when allowing employers to obtain information on the personal and private lives of its applicants and employees. The most effective way to balance these rights and interests is to require notice, authorization, and disclosure.

As discussed in Section III, the Fair Credit Reporting Act establishes broad definitions of the terms “consumer reporting agency,” “consumer report,” and “investigative consumer report.” At least one circuit has interpreted the definition of

⁶⁵ FCRA § 606(a)(1)(B), 15 U.S.C. § 1681d(a)(1)(B).

⁶⁶ FCRA § 606(a)(2), 15 U.S.C. § 1681d(a)(2).

⁶⁷ FCRA § 606(b), 15 U.S.C. § 1681d(b).

⁶⁸ FCRA §§ 616, 617, 15 U.S.C. § 1681(n-o) (2000).

“consumer report” broadly, giving wide range to what may qualify.⁷⁰ Apparently, courts interpret these definitions in such a way as to comport with the consumer protection purposes of the FCRA.⁷¹

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 ways to investigate their candidates.

Until now, employers have relied upon third party consumer reporting agencies to compile information on individuals. But now, as online social networking searches prove a much quicker and less expensive means of obtaining the kind of information that an employer previously relied upon someone else to obtain, no statutory buffer exists to filter that information and ensure its fairness, relevancy, and accuracy. If expanded to cover these new online background checks, the FCRA would provide that adequate buffer to hold employers accountable and to help ensure that their decisions are based on fair, relevant, and accurate information.

A. Distinguishing Between Social Networks and Other Online Information Outlets

The first step in expanding these definitions of the FCRA would be to distinguish between social networking services and other information outlets on the web. What makes online social networking services different enough from other sources of online information to justify covering only these services and not every information source on the internet? The answer lies in three primary differences between online social

⁶⁹ FCRA § 619, 15 U.S.C. § 1681(q) (2000).

⁷⁰ Reynolds v. Hartford Fin. Servs. Group, Inc., 435 F.3d 1081, 1094 (9th Cir. 2006).

networking services and other online information outlets such as blogs, “webzines” and online newspapers: intent, purpose and expectation—all three of which are linked.

The target audience for which the information has been provided represents a key difference between social networking services and other information outlets. While the nature of the World Wide Web may allow the general public access to MySpace profiles, the profiles’ creators intend their use and accessibility only for members of their MySpace social networks and not for the general public. Other information sources, such as blogs, online newspapers, and online magazines, publish information for a general public purpose. The attitude that many have expressed as the online social networking debate heats up (namely, that people should just “watch what they say” on their MySpace profile), could chill free speech and associational rights, rights that Americans now exercise through their online profiles.⁷² Employees should not carry the burden of “watching what they say,” rather, employers should carry the burden of “watching what they do” with that information.

Online newspaper and magazine articles often feature individuals who have been given an opportunity to offer the best information about them as possible, with the important understanding of the very public nature and purpose of such articles. John Doe, contacted by the Daily Times to provide information about his life and his background for a human interest piece on community leaders, has been put on notice that

⁷¹ Id.

⁷² This kind of attitude supports and protects the legal status quo with respect to online social networking and employment screening. While this current body of law does not explicitly ban speech or association, it could have the continued effect of implicitly stifling the legitimate speech and associational rights of online social networking users. The Supreme Court expressed its concern over the “chilling effect” that some laws can have on First Amendment rights in the case of *Lamont v. Postmaster General*, 381 U.S. 301 (1965). In that case, the Court invalidated a federal law requiring postal patrons to specifically authorize the delivery of every piece of mail that might have been considered communist political propaganda.

his information will be broadcast publicly for a general informational purpose. He will likely select information carefully that portrays him in a favorable light to the public eye, including potential employers.

While blogs fall somewhere in between online newspapers and online social networking websites, they still represent a source of information that has a general public purpose. Bloggers generally write intending to provide information and present different viewpoints on various issues to the general public. Because bloggers write with an informational purpose and a public audience in mind, rather than with a social purpose and limited private audience in mind, this article does not advocate for the expansion of the FCRA to cover blogs.

When an individual creates a MySpace profile, however, she creates a profile of herself clearly meant for use within a private social community, a community whose membership requires an invitation. Accordingly, it may be more light-hearted and less serious. MySpace social networks represent the online equivalent of social clubs or social gatherings; their members do not expect employers to use them as tools to secretly watch members' private lives. MySpace members write their profiles with a social purpose and limited audience in mind.

The FCRA's purpose reaches information that may create an inaccurate or unfair portrayal of the candidate for employment purposes. Because using information found on social networking profiles for employment purposes increases the risk of making an unfair decision based upon irrelevant, unfair, or inaccurate information, the FCRA should

While the invalidated law did not explicitly ban the propaganda, it could have had the effect of stifling it by placing upon its recipients an onerous burden.

cover only online social networking services and not all information generally available about a candidate on the internet.

Giving definitional boundaries to the term “social networking service” for the purposes of the FCRA will become important to avoid assigning legal liability to an endless and vast array of online entities. Keeping in mind the reasons for extending the FCRA to cover social networking services, this new definition should be formulated in terms of social networking services’ purpose and function. If the purpose of an online service is, as MySpace has stated it, to create a private community through which members can communicate and network, the FCRA should consider it a social networking service. The Federal Trade Commission, which enforces the FCRA⁷³, can provide administrative guidance as to what websites comprise the body of social networking services on the web.

B. Amending the FCRA

One of the most attractive options in considering an amendment to the FCRA is simply to amend two key definitions—“consumer reporting agency” and “investigative consumer report”—and to add one more: “social networking service.” Legal counsel for the Federal Trade Commission would seem best suited to recommend specific draft statutory language for an amendment. However, for purposes of fostering discussion on a concrete proposal, this article proposes such language.

Sections (e) and (f) of 15 U.S.C. §1681a follow, with proposed changes in italics:

(e) The term "investigative consumer report" means a consumer report or portion thereof in which *information on a consumer's character, general reputation, personal characteristics, or mode of living, is obtained through:*

⁷³ FCRA § 621(a)(1), 15 U.S.C. § 1681s(a)(1) (2000).

1) personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information; *OR*

2) *an online social networking service described in part (f)(2) of this subsection.*

However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

(f) The term "consumer reporting agency" means:

1) any person which, for monetary fees, dues, or on a cooperative nonprofit basis, 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, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports; *OR*

2) *any online social networking service that electronically stores and displays personal information entered through individual online social networking profiles maintained and edited by its users, members, or subscribers, for the purpose and function of personal use in social networking, communication, information-sharing or other foreseeable aspects of online social networking.*

A new subsection (g) of 15 U.S.C. §1681a, defining “online social networking service” would state that:

(g) The term “online social networking service” means any website or other world wide web-based service that exists and functions for the purpose of allowing its users, members, or subscribers to create, maintain, use, or edit private social networks or personal profiles containing information provided for a social purpose.

An amendment to the FCRA should also include a provision to except these social networking websites from the provisions of the FCRA that have no relevance to employment. Such an exception would preclude social networking websites from the

requirements of parts of the FCRA that do not govern employment background checks.⁷⁴

A new 15 U.S.C. §1681a(g)(1) would state that the term “online social networking service”:

(1) applies only to the provisions of this Act that govern the access and use of consumer information by employers.

Expanding the definitions section of the FCRA to reach online social networking providers such as MySpace and Facebook will update a law that has provided very necessary and important protections for employees. The Fair Credit Reporting Act, as amended to cover online social networking, will continue to provide the necessary balance between employer and employee rights. It will create accountability for the employer to ensure that employment decisions continue to be based upon fair, accurate, and relevant information about applicants and employees and provide civil remedies to the aggrieved.

V. CONCLUSION

Where the internet has expanded into “places” where one may have a reasonable expectation of privacy, the fundamental meaning of privacy still remains the same. American employees still expect privacy in their off-duty lives, whether they conduct their social lives in traditional ways or through new ways, such as online social networking. The current debate regarding online social networking and employment decisions should not focus on whether millions of people *can* access information about individuals online; it should focus on the acceptable and permissible uses of that information. The very nature of the internet permits vastly greater degrees of public access to information. After all, the age in which Americans now live has been dubbed

⁷⁴ Only FCRA § 604, and to some extent § 606, deal with consumer reporting in the context of employment

the Information Age. However, Americans conducting their lives in this Information Age will find it increasingly difficult to hide information about themselves behind physical walls. Therefore, thinking about privacy should involve thinking about how to filter that information to ensure its proper and acceptable uses.

Because searches of online social networking services only stand to become more prevalent and popular among employers, Congress should expand the Fair Credit Reporting Act to ensure employees that use these websites adequate protection from unfair, illegal or arbitrary employment decisions. The original purposes of the FCRA accommodate its expansion to cover the situation of the employer searching online social websites for a candidate or employee's online social networking profile. Employers will benefit from such an expansion of legal protections because, while retaining the rights and privileges of access to online information about candidates and employees, an amended FCRA will hold them accountable to make fair and efficient employment decisions based upon accurate, reliable, and relevant information. This solution effectively strikes an agreeable balance between an employer's right to know its candidates and employees and an employee's right to privacy and fair employment decision making.

screening. Almost all of the rest of the Fair Credit Reporting Act governs traditional credit reporting.