University of Michigan Journal of Law Reform

Volume 48

2015

Social Media and the Job Market: How to Reconcile Applicant Privacy with Employer Needs

Peter B. Baumhart
University of Michigan Law School

Follow this and additional works at: https://repository.law.umich.edu/mjlr

 Part of the Internet Law Commons, Labor and Employment Law Commons, and the Privacy Law Commons

Recommended Citation

Peter B. Baumhart, *Social Media and the Job Market: How to Reconcile Applicant Privacy with Employer Needs*, 48 U. MICH. J. L. REFORM 503 (2015).
Available at: https://repository.law.umich.edu/mjlr/vol48/iss2/5

This Note is brought to you for free and open access by the University of Michigan Journal of Law Reform at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in University of Michigan Journal of Law Reform by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

SOCIAL MEDIA AND THE JOB MARKET: HOW TO RECONCILE APPLICANT PRIVACY WITH EMPLOYER NEEDS

Peter B. Baumhart*

In the modern technological age, social media allows us to communicate vast amounts of personal information to countless people instantaneously. This information is valuable to more than just our "friends" and "followers," however. Prospective employers can use this personal data to inform hiring decisions, thereby maximizing fit and minimizing potential liability. The question then arises, how best to acquire this information? For job applicants, the counter-question is how best to protect the privacy of their social media accounts. As these two competing desires begin to clash, it is important to find a method to mediate the conflict. Existing privacy law, whether rooted in constitutional, statutory, or common law, is insufficient to cope with the practice, and pending legislation also fails to adequately account for the legitimate interests of both parties. This Note advocates a novel solution: a modified information escrow that would provide employers with the relevant information they seek while keeping private the substantive content of applicants' social media accounts.

INTRODUCTION

When people tweet, upload pictures, or post status updates, they are not likely thinking about the long-term effects of those actions. We live in an age, however, of near-instantaneous communication accompanied by the capacity to indefinitely store electronically transmitted data; those effects are real and have the potential for serious and unanticipated consequences down the road. In particular, social media activity is increasingly becoming an object of interest to employers, who are attempting to expand the pool of information from which they can learn about potential employees.

This Note explores the developing employer practice of requesting or requiring that applicants provide access to the private information located on their social media accounts. In doing so, this Note acknowledges the legitimate interests of each party to the hiring decision—the applicant and the employer—and seeks to articulate a solution that accommodates the needs of each. Part I will explain the practice at issue and examine the problems that necessarily arise. Part II will canvass the state of the law as it pertains (or

* J.D. Candidate (2015), University of Michigan Law School. The author would like to thank Emily Brown, M. Jeanette Pitts, and Michael Powers for their helpful feedback and suggestions. The author would especially like to thank Professor J.J. Prescott, whose guidance was indispensable throughout the process of researching and writing this Note.

might pertain) to the problems raised in Part I. Part III will describe the shortcomings of the current law and present an alternative solution: a modified information escrow that recalibrates the budget of available information between the applicant and the employer to maximize the net payoff for both parties.

I. EMPLOYERS, APPLICANTS, AND SOCIAL MEDIA

The use of social networking sites (SNSs) is more popular than ever, with over sixty-seven percent of Internet users having some form of social media presence.[1] Facebook alone had 1.32 billion active monthly users at the end of June 2014.[2] But by posting personal information online, SNS users risk communicating that information to more than just their friends—tweets, status updates, pictures, and the like can provide a veritable treasure chest of information to teachers, co-workers, strangers, and, most importantly for this Note, potential employers. Although statistics regarding the frequency with which employers actually look at an applicant's SNS profiles vary widely,[3] the trend is unquestionable, indicating that an applicant's SNS account content appears to be fair game for employers. This may not seem so troubling when the prospective employer is simply viewing information that the applicant has made public; some employers, however, are demanding applicants' passwords to view otherwise unavailable, private information.[4] In today's

1. MAEVE DUGGAN & JOANNA BRENNER, PEW RESEARCH CTR., THE DEMOGRAPHICS OF SOCIAL MEDIA USERS – 2012 3 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2013/PIP_SocialMediaUsers.pdf. *Compare id.* (showing social media use by age as eighty-nine percent of users ages eighteen to twenty nine, seventy-seven percent of users ages thirty to forty-nine, fifty-two percent of users fifty to sixty-four, and thirty-two percent of users sixty-five and older), *with* AMANDA LENHART ET AL., PEW RESEARCH CTR., SOCIAL MEDIA & MOBILE INTERNET USE AMONG TEENS AND YOUNG ADULTS 17 (2010), *available at* http://web.pewinternet.org/~/media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf (indicating that social media use by Internet users was seventy-two percent of users ages eighteen to twenty-nine and forty percent of users age thirty and older in 2009).

2. *Company Info*, FACEBOOK, http://newsroom.fb.com/company-info/ (last visited Oct. 8, 2014).

3. The research on this statistic shows frequency of use ranging from approximately forty percent of employers to over ninety percent of employers. *Compare* Mary Lorenz, *Two in Five Employers Use Social Media to Screen Candidates*, CAREERBUILDER (July 1, 2013), http://thehiringsite.careerbuilder.com/2013/07/01/two-in-five-employers-use-social-media-to-screen-candidates/ (claiming that thirty-nine percent of employers use social media to screen applicants), *with* JOBVITE, 2013 SOCIAL RECRUITING SURVEY RESULTS 8 (2013), *available at* http://web.jobvite.com/rs/jobvite/images/Jobvite_2013_SocialRecruitingSurveyResults.pdf (claiming that ninety-three percent of recruiters are likely to use an applicant's SNS profile).

4. *See, e.g.*, Mark B. Gerano, Note, *Access Denied: An Analysis of Social Media Password Demands in the Public Employment Setting*, 40 N. KY. L. REV. 665, 672–73 (2013) (describing the

competitive job market, applicants may not be in a position to refuse.[5]

A. Social Networking Sites (SNSs): Content and Use

The term "social networking" or "social media" encompasses a wide range of websites, among them Facebook, Twitter, and Instagram. Though the specific functions and capabilities of these sites may differ, at its core a social networking site is "a website that is designed to help people communicate and share information, photographs, etc. within a group."[6] Through accounts on various SNSs, users are able to connect with friends, receive updates on local and global events, and communicate thoughts and beliefs with others.[7] One of the most common features of SNSs is the user's profile, an individual's unique webpage where the user can post personal details (e.g., age, sex, place of residence) and share photographs, messages, and other such information.[8] For example, a standard Facebook profile allows a user to share "posts," photos, apps, and the like, all in the name of expressing "who [the user is] through all the things [she does]."[9]

As users post ever-increasing amounts of personal information online, the risk that an unauthorized party may access damaging information increases. Once it is posted online, anyone able to access a user's information can download it, including search engines that simply store the information indefinitely.[10] Thus, deleting information from an SNS account does not necessarily purge that

---

Maryland Department of Corrections' 2011 policy of requiring prison guard applicants to provide their SNS passwords to the Department). *But see* Shel Israel, *The Great Facebook Employee Password Non-Issue*, FORBES (Mar. 25, 2012, 8:32 PM), http://www.forbes.com/sites/shelisrael/2012/03/25/the-great-facebook-employee-password-nonissue/ (arguing that the frequency with which employers actually require disclosure of SNS account passwords has been overstated).

5. Shannon Mcfarland, *Job Seekers Getting Asked for Facebook Passwords*, USA TODAY (Mar. 21, 2012, 10:56 AM), http://usatoday30.usatoday.com/tech/news/story/2012-03-20/job-applicants-facebook/53665606/1 ("[J]ob applicants are confronting [requests to provide access to their SNS profiles], and some of them cannot afford to say no.").

6. *Social Networking Site Definition*, CAMBRIDGE DICTIONARIES ONLINE, http://dictionary.cambridge.org/us/dictionary/business-english/social-networking-site (last visited Oct. 8, 2013).

7. *Company Info*, *supra* note 2.

8. *See* Ian Byrnside, Note, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 453 (2008).

9. *Introducing Timeline*, FACEBOOK, https://www.facebook.com/about/timeline (last visited Nov. 9, 2013).

10. *See Information Is Permanent*, IKEEPSAFE, http://www.ikeepsafe.org/be-a-pro/reputation/information-is-permanent/ (last visited Oct. 8, 2014).

information completely. Oftentimes, though, users will be able to control access to their information using the SNS's privacy settings.[11] For instance, Facebook users can decide who views the content of their profiles on a case-by-case basis (i.e., every time they post something, users can select the audience who will be able to view that content).[12] But users may be overestimating the privacy protection that such controls actually provide: combining the potential permanency of downloadable online content with complicated procedures to set privacy controls could mean that "private" information is actually quite public.[13]

SNSs are different both in degree and in kind from previous communication technologies. No prior technology was capable of the instantaneous and mass communication that SNSs offer, and the information that SNSs convey is susceptible to surveillance and permanent storage in ways previously unimagined.[14] In short, SNS users are able to communicate more information to more people but have less hope of defending that information from prying eyes. Thus far, the long-term privacy impacts are undetermined. The very fact that such vast quantities of personal information are so easily accessible may increase the perceived imperative for certain entities, such as employers, to monitor (potential) employees' SNS use to avoid future liability.[15] Moreover, the increasing ubiquity of SNSs makes it impractical not to have some sort of social media presence. Any impingement on the privacy of online information will, therefore, necessarily affect a considerable segment of the population. Hence, the developing employer practice of requesting access to job applicants' SNS accounts could have far-reaching implications, especially as those who have grown up using SNSs begin to enter the workforce *en masse*.

---

11. Byrnside, *supra* note 8, at 453–54; *see also* Lindsay S. Feuer, Note, *Who is Poking Around Your Facebook Profile?: The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites*, 40 HOFSTRA L. REV. 473, 485–87 (2011) (describing Facebook's privacy settings); *Data Use Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last updated Nov. 15, 2013).

12. *Data Use Policy*, *supra* note 11.

13. *See* Nathan J. Ebnet, Note, *It Can Do More than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, 97 MINN. L. REV. 306, 316–17 (2012); Feuer, *supra* note 11, at 487; *Data Use Policy*, *supra* note 11 (indicating that some information, including the user's name, profile picture, and gender, is "always public").

14. *See* Saby Ghoshray, *Employer Surveillance Versus Employee Privacy: The New Reality of Social Media and Workplace Privacy*, 40 N. KY. L. REV. 593, 597 (2013) (comparing SNSs to telephones).

15. *See id.* at 597 ("[E]ase of instant communication and access to its stored content within social media may provide [a] stronger rationale for surveillance.").

B. Employers' Pre-Screening Use of SNSs: Reasons and Risks

When making hiring decisions, employers use a variety of tools such as résumés, references, and interviews. In recent years, employers have also made use of online searches to vet applicants.[16] The next logical step is investigating applicants' SNS accounts, which some employers are already doing.[17] If the employer is limited to only the information that an applicant has made publicly available on an SNS, then there would be little to distinguish from a standard online search. Moreover, an applicant cannot reasonably expect that information made publicly available will remain protected from anyone, including prospective employers.[18] A more invasive practice appears to be emerging, however: requesting access to the applicant's private SNS account information.[19]

An employer can gain access to an applicant's SNS accounts in several ways: (1) the employer may directly ask the applicant to turn over her password[20] or log the employer in to her account; (2) the employer may request that the applicant add the employer's (or an agent's) SNS account as a contact, or "friend," to allow the employer to see the applicant's SNS account content; or (3) the employer may use more surreptitious means, such as requesting an authorized viewer of the applicant's SNS content to share that content with the employer.[21] Though the method of gaining access may make a difference regarding the amount of private information the employer is able to acquire,[22] any of these methods will usually provide the employer with more private information than would be otherwise available.

---

16. Allan Hoffman, *Job Applicant, Beware: You're Being Googled*, MONSTER.COM, http://career-advice.monster.com/job-search/getting-started/hr-googling-job-applicants/article.aspx (last visited Oct. 8, 2014) (describing that, as early as 2006, seventy-seven percent of employers were using online search engines to research applicants).

17. *See* Lorenz, *supra* note 3.

18. *See* Hoffman, *supra* note 16.

19. *See* Sara Gates, *CISPA Amendment Banning Employers from Asking for Facebook Passwords Blocked*, HUFFINGTON POST (Apr. 21, 2013, 9:46 PM), http://www.huffingtonpost.com/2013/04/21/cispa-amendment-facebook-passwords-blocked_n_3128507.html (discussing the defeat of an amendment to the Cyber Intelligence Sharing and Protection Act that would have banned employers from requesting SNS account passwords); *Resume, Cover Letter, and Your Facebook Password?*, NPR (Mar. 21, 2012, 3:00 PM), http://www.npr.org/2012/03/21/149091139/resume-cover-letter-and-your-facebook-password (interview with Robert Collins, an applicant to the Maryland Department of Public Safety and Corrections who had to provide his SNS account password as part of his application).

20. *E.g., Resume, Cover Letter, and Your Facebook Password?*, *supra* note 19.

21. *See, e.g.*, Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 WL 6085437, at *1 (D.N.J. July 25, 2008).

22. Using Facebook messages as an example, only the account user and the recipient of a message will be able to view a user's Facebook messages. *Who Can See My Messages?*,

While accessing an applicant's SNS account may seem to be an unwarranted invasion of privacy, there are many incentives for an employer to conduct as thorough a pre-screening process as possible. Pre-employment screening can result in better employees (in terms of productivity, honesty, and turnover rate),[23] reduced non-violent employee misconduct,[24] and a reduced risk of negligent hiring liability.[25] Certain employers also have to consider whether an applicant can be trusted with sensitive information or trade secrets,[26] and looking at the applicant's SNS account can provide insight into the type of information that the applicant tends to post online. At the most basic level, pre-employment screening helps to ensure that the applicant "appears professional and will fit in with company culture."[27] Applicants' SNS accounts would seem to be highly relevant to this analysis, considering that one of the major purposes of SNSs is to enable the user to "express who [she is]."[28] Moreover, SNSs are a cost-effective pre-screening tool—searches can be conducted quickly and in-house.[29]

SNSs can be a powerful pre-screening resource, but employer use of such information also carries certain risks. Applicants' SNS accounts often contain information that employers are forbidden from considering when making hiring decisions, such as age, race,

---

FACEBOOK, https://www.facebook.com/help/www/212388195458335?rdrhc (last visited Oct. 8, 2014). Thus, an employer would only be able to view an applicant's messages through direct access to the applicant's account, but not by adding the applicant as a "friend" or any of the other methods.

23. ALAN KINSEY, INQUIREHIRE, THE BENEFITS OF PRE-EMPLOYMENT SCREENING 2 (n.d.), *available at* http://www.sweeneyinc.com/files/benefits_preemployment_screening.pdf (last visited Nov. 9, 2013). Inquirehire is a consulting firm that offers hiring solutions for business, government, and non-profit organizations.

24. *Id.* at 3.

25. *Id.* at 3–4; *see also* Alissa Del Riego et al., *Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy*, 16 J. INTERNET L. 1, 18 & n.9 (2012).

26. *See* Alexander Naito, Comment, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. PA. J. CONST. L. 849, 863 (2012); *see also* Ghoshray, *supra* note 14, at 593–94 (discussing a hypothetical situation where an employee posts trade secrets on an SNS).

27. Leslie Kwoh, *Beware: Potential Employers are Watching You*, WALL ST. J. (Oct. 29, 2012), http://online.wsj.com/news/articles/SB10000872396390443759504577631410093879278.

28. *Introducing Timeline*, *supra* note 9; *see also Getting Started with Twitter*, TWITTER, https://support.twitter.com/groups/50-welcome-to-twitter/topics/204-the-basics/articles/215585-getting-started-with-twitter# (last visited Oct. 8, 2014) (explaining that one of the purposes of Twitter is to help users "find [their] own voice and show others what [they] care about").

29. Ebnet, *supra* note 13, at 319 (describing how, in contrast to criminal history background checks or credit reports, an employer need not use a third-party reporting company to research an applicant's social media history).

and sex.[30] Employer access to such information could lead to discrimination claims if the applicant is not hired. Requiring that applicants disclose password information will also likely violate the SNS's terms of service,[31] which could expose both the applicant and the employer to liability.[32] Because of the nature of SNSs (i.e., that the user is selectively creating an online persona), the information contained therein is also highly susceptible to concerns regarding accuracy and authenticity.[33] Additionally, requesting access to an applicant's private SNS content could foster an environment of distrust and create tension between the applicant and the employer that persists after an employee is hired.[34]

A recent poll indicates approximately forty percent of employers research applicants' SNS accounts as part of employment pre-screening,[35] up from about twenty-seven percent in 2006.[36] As long as SNSs remain popular among applicants, it is fair to believe that employers will continue to utilize them in the pre-screening process. Requesting access to private content on applicants' SNS accounts will allow employers to maximize the amount of information available, and it appears applicants can do very little to resist if they hope to be hired.[37] In a competitive market, many applicants

---

30. Byrnside, *supra* note 8, at 462–63; *see also* Kwoh, *supra* note 27 ("By going online, employers expose themselves to all kinds of information that cannot be legally considered in the hiring process, such as religion, gender, and health status.") (quoting Max Drucker, CEO Of Social Intelligence Corporation, a business which screens job applicants on behalf of employers).

31. Facebook officials have already taken a stand on this issue, indicating that requiring a job applicant to disclose her password constitutes a violation of the site's terms of service. *See* Erin Egan, Chief Privacy Officer, *Protecting Your Passwords and Privacy*, FACEBOOK (Mar. 23, 2012, 8:32 AM), http://www.facebook.com/note.php?note_id=326598317390057 ("As a user, you shouldn't be forced to share your private information and communications just to get a job. . . . That's why we've made it a violation of Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password.").

32. *See id.* (stating that Facebook will "take action to protect the privacy and security of [its] users . . . by initiating legal action"); Byrnside, *supra* note 8, at 468 (discussing potential employer liability under the Computer Fraud and Abuse Act resulting from violation of SNS terms of service).

33. Byrnside, *supra* note 8, at 470–71; *see also* Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and the Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 562 (2013) ("[S]ocial networking sites may contain a wide range of information, digital exchanges, personal musings, and retorts that a potential screener may take out of context.").

34. *See* Scott Brutocao, *Issue Spotting: The Multitude of Ways Social Media Impacts Employment Law and Litigation*, 60 THE ADVOCATE (TEX.) 8, 10 (2012) ("[E]mployees do not like perceived intrusions on their privacy.").

35. Lorenz, *supra* note 3.

36. Byrnside, *supra* note 8, at 457 (reporting a poll conducted by the National Association of Colleges and Employers that surveyed 254 employers).

37. *See, e.g.*, Mcfarland, *supra* note 5.

cannot afford to take themselves out of the running for a job, even if they would prefer not to share such private information.

Ultimately, in an effort to obtain as much pertinent information as possible, employers may request (indeed, some already do) access to the private content of applicants' SNS accounts. In the absence of legal protections, applicants have few options other than to capitulate to such requests. Part II will examine the current state of the law and whether any such protections exist.

II. SQUARE PEG, ROUND HOLE: SOCIAL MEDIA AND THE LAW

The law has had a difficult time adapting to the advent of SNSs. This in turn, has created significant confusion surrounding issues like employers' requests for access to applicants' SNS accounts. Critics of this practice have proposed several solutions, including extending the protections of the Fourth Amendment to cover public employees' SNS accounts,[38] reforming federal legislation such as the Stored Communications Act,[39] or mandating third-party searches to bring them under the aegis of the Fair Credit Reporting Act.[40] Congress has considered several proposals that would ban employers from requesting applicants' SNS account passwords,[41] but has yet to pass legislation on the subject. On the other hand, several state legislatures have enacted laws barring the practice,[42] but such legislation remains relatively rare.[43] Even where it exists, this legislation fails to adequately address the issue because it bans the practice outright, thereby ignoring employers' legitimate interests in acquiring certain information contained on applicants' SNS accounts. Constitutional and common law protections are also insufficient to cope with this practice.[44] This Part will explore the state

38. Naito, *supra* note 26, at 854.

39. Feuer, *supra* note 11, at 476.

40. Ebnet, *supra* note 13, at 309.

41. *E.g.*, Social Networking Online Protection Act, H.R. 537, 113th Cong. (2013) (currently referred to committee); Password Protection Act of 2013, H.R. 2077, 113th Cong. (2013).

42. *E.g.*, ARK. CODE ANN. § 11-2-124 (2013). *See also infra* Part II.B.2.

43. Only sixteen states have enacted legislation that prohibits employers from requesting access to applicants' or employees' private SNS account information. *See Employer Access to Social Media Usernames and Passwords: 2012 Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 17, 2013), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx (stating that six states enacted such legislation in 2012); *Employer Access to Social Media Usernames and Passwords 2013*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last updated Sept. 28, 2014) (stating that ten states enacted such legislation in 2013).

44. *See infra* Part II.A.

of the law as it exists and demonstrate that SNSs fit uncomfortably into a legal framework that is struggling to keep pace with the times.

A. Constitutional and Common Law Privacy

The state of the law regarding privacy in the employer-applicant relationship is far from settled. As it stands, some courts have ruled that applicants enjoy the same expectation of privacy as their employee counterparts.[45] Far more common, however, is the notion that applicants are entitled to a diminished expectation of privacy as compared to employees.[46] The best-case scenario for an applicant's right to SNS account privacy can thus be determined by examining an employee's right to the same. Existing privacy law does not adequately protect even an employee's SNS information from an employer's review; therefore, an applicant also cannot claim that the practice of requesting access to the applicant's SNS account violates a privacy right.

Both the common law, through an intrusion on seclusion claim,[47] and the United States Constitution, through the Fourth Amendment,[48] provide protection to public employees, while only the common law protects the privacy of private employees. In either circumstance, the employee must demonstrate that she has a

---

45. *See, e.g.*, Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 83–85 (Cal. Ct. App. 1991) ("Our review . . . satisfies us that the voters did not intend to grant less privacy protection to job applicants than to employees."). *Soroka* has no precedential value, however, because the parties settled out of court, and the case was subsequently dismissed as moot. Soroka v. Dayton Hudson Corp., 862 P.2d 148 (Cal. 1993). In any event, this part of *Soroka*, while not explicitly overruled, is likely dead in light of *Loder v. City of Glendale*, 927 P.2d 1200, 1222 (Cal. 1997), which held that "drug testing of all job applicants is constitutionally permissible under the Fourth Amendment even though similar drug testing of current employees seeking promotion is not." *See also* Georgia Ass'n of Educators v. Harris, 749 F. Supp. 1110, 1113–15 (N.D. Ga. 1990) (applying precedent based on privacy expectations of employees to applicants).

46. *See, e.g.*, Wilkinson v. Times Mirror Corp., 264 Cal. Rptr. 194, 203 (Cal. Ct. App. 1989) ("Any individual who chooses to seek employment necessarily also chooses to disclose certain personal information to prospective employers . . . and to allow the prospective employer to verify that information."). It should be noted that both *Soroka* and *Wilkinson* rested on interpretations of California's state constitution, which contains an express right to privacy. *See* CAL. CONST. art. I, § 1.

47. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977) (articulating the "intrusion on seclusion" invasion of privacy tort).

48. *See* U.S. CONST. amend. IV. The Fourth Amendment does not apply to searches conducted by private parties, such as private employers. *See* Walter v. United States, 447 U.S. 649, 656 (1980).

reasonable expectation of privacy.[49] If the court finds that a public employee has a reasonable expectation of privacy, it must then determine whether the employer's search was reasonable.[50] For an employee to prevail upon an intrusion on seclusion claim, the employee must demonstrate a subjective expectation of privacy in addition to an objectively reasonable expectation.[51] The employee must also show that the intrusion would be "highly offensive to a reasonable person."[52]

1. Reasonable Expectation of Privacy

The Supreme Court has not yet spoken to the issue of whether the Fourth Amendment grants employees a reasonable expectation of privacy in SNS accounts. The Court has, however, examined whether employees have a reasonable expectation of privacy in arguably related areas. In *O'Connor v. Ortega*, a Fourth Amendment case, the Supreme Court relied on two alternative tests to determine whether an employee had a reasonable expectation of privacy from a state employer in his personal office. The first test, articulated in the plurality opinion, determines the employee's privacy expectation "in the context of the employment relation."[53] That is, the plurality test requires a "case-by-case" assessment of whether the area in which a privacy expectation is claimed is "so open to fellow employees or the public that no expectation of privacy is reasonable."[54] The second test, posited by the concurrence, would simply apply Fourth Amendment protections to all government offices "as a general matter."[55] In other words, the concurrence would find that employees have a reasonable expectation of privacy in their offices as a general rule.

---

49. Smith v. Maryland, 442 U.S. 735, 740 (1979) ("[A]pplication of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."); Kline v. Security Guards, Inc., 386 F.3d 246, 260 (3d Cir. 2004) (stating that the intrusion on seclusion cause of action "requires that the plaintiff have a reasonable expectation of privacy"); *see also In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257–58 (S.D.N.Y. 2005) (adapting the reasonable expectation of privacy test established in O'Connor v. Ortega, 480 U.S. 709 (1987), to the private employment context).

50. *O'Connor*, 480 U.S. at 719–20.

51. Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc., 306 F.3d 806, 812–13 (9th Cir. 2002). Because the subjective expectation element turns simply on whether the employee had an expectation of privacy in fact, this Note will not examine it in detail.

52. *Id.* at 812.

53. *O'Connor*, 480 U.S. at 717.

54. *Id.* at 718.

55. *Id.* at 731 (Scalia, J., concurring).

In the most recent case addressing the issue of employee expectations of privacy, dealing with personal text messages sent from an employer-issued pager, the Supreme Court declined to clarify which test controls.[56] Instead, the Court assumed that the employee had a reasonable expectation of privacy against his public employer under either test before inquiring as to the reasonableness of the employer's invasion of that privacy expectation.[57] The Court expressly avoided passing judgment concerning employees' privacy expectations regarding electronic communications,[58] thus providing minimal guidance for analyzing the question of SNS accounts. By assuming that the employee had a reasonable expectation of privacy, the Court also avoided the fact that the *O'Connor* tests are poorly suited to issues of cyber-privacy: the focus on a physical space (e.g., an office) and third-party incursions therein does not translate well into the ethereal realm of the Internet.[59]

There are several factors to consider when assessing the reasonableness of a privacy expectation. One such factor is the legality of the search at issue.[60] According to the Department of Justice, it is a federal crime to access an individual's SNS account in violation of the SNS's terms of service.[61] Requiring an applicant to disclose an SNS account password constitutes such a violation;[62] however, the DOJ has indicated that it will not prosecute these offenses.[63] Consequently, it is not clear exactly what effect this factor will have on the reasonableness of privacy expectations in SNS accounts. In addition to legality, employer policies play an important role in determining the reasonableness of privacy expectations. Employees cannot have a reasonable expectation of privacy in electronic communications if

---

56. City of Ontario v. Quon, 560 U.S. 746, 756 (2010).

57. *Id.* at 759–60.

58. *Id.* at 757–60.

59. *See* Del Riego et al., *supra* note 25, at 18 (discussing the obsolescence of American privacy law in the digital realm); Naito, *supra* note 26, at 872–73 (same).

60. *See* Florida v. Riley, 488 U.S. 445, 450–51 (1989). In *Riley*, the police conducted a helicopter flyover of the defendant's property, during which they observed a marijuana greenhouse. The Court held that this flyover did not constitute a search because the defendant "could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing aircraft." *Id.* The Court also noted that it would be "a different case if flying at that altitude *had been contrary to law or regulation*." *Id.* at 451 (emphasis added).

61. Mcfarland, *supra* note 5.

62. *See supra* note 31 and accompanying text; *see also Revealed: How Colleges and Employers Ask for Candidates' Facebook and Email Passwords During Job Interviews*, DAILY MAIL (Mar. 6, 2012, 12:14 PM), http://www.dailymail.co.uk/news/article-2111059/Colleges-jobs-asking-Facebook-email-passwords-job-interviews.html?ito=feeds-newsxml (discussing a Facebook spokesman's comments that Facebook "prohibit[s] anyone from soliciting the login information or accessing an account belonging to someone else").

63. Mcfarland, *supra* note 5.

it is the employer's policy to monitor such communications[64] and the employee has notice of the policy.[65] Whether the communications occurred through channels furnished by the employer is also relevant to the privacy analysis, with courts routinely holding that employees can have no reasonable expectation of privacy in such channels.[66] Finally, if an employee has given her employer access to an SNS account, it may also be important whether the employee provided the access freely or whether the access was coerced.[67]

Lower courts have struggled when deciding whether SNS users have a reasonable expectation of privacy in their accounts. Some courts, focusing on factors such as exposure of the information to the public, or even to a large group of privately-selected followers, have found that such information cannot be considered private.[68] Other courts, relying instead on steps taken to limit third-party access to SNS content, have found that employees can plausibly claim a reasonable expectation of privacy in that content.[69] Decisions regarding the discoverability of information on SNS accounts also fall on both sides of the line,[70] illustrating the difficulties that courts

---

64. *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of [his employer's] Internet policy."); *see also* Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (upholding private employer's search of employee's laptop based on employer's policy to search the laptops).

65. *See Simons*, 206 F.3d at 398 n.8.

66. *See, e.g., Muick*, 280 F.3d at 743 ("The laptops were [the employer's] property and it could attach whatever conditions to their use it wanted to."); *see also* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 559 (S.D.N.Y. 2008) (finding that employer's policy to monitor emails sent on "company equipment" did not extend to emails sent via third-party services like Google without evidence that the employee utilized the employer's computers).

67. *See, e.g.,* Pietrylo v. Hillstone Restaurant Group, No. 06-5754, 2008 WL 6085437, at *4 (D.N.J. July 25, 2008) (finding that an implicit threat of negative employment consequences could constitute coercion to provide access to employee's private website); *see also* Del Riego et al., *supra* note 25, at 20 (collecting cases under the federal Stored Communication Act (SCA) indicating that an employer's coercion to gain access to an employee's SNS may void the employee's consent to the employer's access).

68. *E.g.,* United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) ("[The defendant's] legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted . . . ."); Maremont v. Susan Fredman Design Group, Ltd., No. 10 C 7811, 2011 WL 6101949, at *7–8 (N.D. Ill. Dec. 7, 2011) (finding that exposure of information to the public and to over 1200 followers defeated any expectation of privacy).

69. *E.g.,* Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 372–74 (D.N.J. 2012) (refusing to dismiss the plaintiff's invasion of privacy claim because she "may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to protect her Facebook page from public viewing"); *Pietrylo*, 2008 WL 6085437, at *7 ("[T]he question of the reasonableness of the Plaintiffs' expectations of privacy is a question of fact for the jury to decide.").

70. *Compare* E.E.O.C. v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434–36 (S.D. Ind. 2010) (social media content partially discoverable), *and* Reid v. Ingerman Smith LLP, No. CV

face with these sorts of issues. Despite this divide, the trend seems to be that courts will not find a reasonable expectation of privacy in SNS accounts.[71]

2. Employer Invasion of Privacy Interest: Reasonable or Highly Offensive?

If a public employee can make the threshold showing of a reasonable expectation of privacy, the issue then becomes whether the employer's invasion of that privacy was reasonable.[72] According to *O'Connor*, this is to be resolved by "balanc[ing] the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace."[73] Public employers have "wide latitude" to enter private offices for "work-related, noninvestigatory purposes"[74] and to conduct "an investigation of work-related employee misconduct,"[75] as long as the search is both justified at its inception and reasonable in its scope.[76] This latitude also extends to a search of an employee's electronic communications made using an employer-provided pager.[77]

Based on the *O'Connor-Quon* line of cases, a public employer's ability to search an employee's SNS account would turn on what qualifies as a work-related purpose and the importance of that purpose when weighed against the employee's privacy interests, which "may be substantial."[78] In *Quon*, the Court relied heavily on the employer's policy of monitoring employee use of computers and other such resources, of which the employee had notice, in determining that the search of the employee's pager communications was reasonable.[79] Such policies are commonplace and often apply to employees' social media use.[80] Consequently, it would seem that as

---

2012-0307, 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012) (relevant social media content discoverable), *with* Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387, 388–89 (E.D. Mich. 2012) (social media content not discoverable). However, in *Tompkins* the court based its decision on a finding that the discovery request was overly broad rather than any expectation of privacy that the plaintiff had in her SNS account. 278 F.R.D. at 388.

71. *See* Feuer, *supra* note 11, at 492–95; Ebnet, *supra* note 13, at 324.
72. *See supra* note 50 and accompanying text.
73. 480 U.S. 709, 719–20 (1987).
74. *Id.* at 723.
75. *Id.* at 725.
76. *Id.* at 725–26.
77. City of Ontario v. Quon, 560 U.S. 746, 761–62 (2010).
78. *O'Connor*, 480 U.S. at 721.
79. *See Quon*, 560 U.S. at 761–62.
80. Naito, *supra* note 26, at 874.

long as a public employer provides notice to its employees of such a policy, the employees' SNS accounts would be fair game for "work-related purposes." As regards applicants for public employment, it is an open question whether employment pre-screening counts as a non-investigative work-related purpose.[81] If so, then notice of the policy would likely be sufficient to insulate the employer's actions; if not, then a search would probably contravene the Fourth Amendment.

Similar to the reasonableness inquiry in the public-employer context, an intrusion on seclusion tort requires that the privacy invasion be conducted "in a manner highly offensive to a reasonable person."[82] An intrusion is highly offensive if it involves "an exceptional kind of prying into another's private affairs."[83] In deciding whether an intrusion is highly offensive, a court should consider "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[84] It is an open question as to what kind of intrusion qualifies as highly offensive, but it is clear that *de minimis* invasions of privacy, such as "[t]he covert videotaping of a business conversation among strangers in business offices," do not qualify.[85]

B. Federal and State Legislation

In addition to the common law and constitutional protections mentioned above, existing federal and state legislation can also protect applicants' privacy in the context of SNS accounts. Some states, responding to the problem that this Note addresses, have passed laws that ban employers from requiring or requesting access to applicants' SNS accounts. Though no such comparable legislation exists at the federal level, several pre-existing federal statutes, such as the Stored Communications Act, have been found to apply to employees' SNS accounts.

---

81. *See* Del Riego et al., *supra* note 25, at 19.

82. Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc., 306 F.3d 806, 812 (9th Cir. 2012).

83. *Id.* at 819.

84. *Id.* (quoting Deteresa v. Am. Broad. Cos., 121 F.3d 460, 465 (9th Cir. 1997)).

85. *Id.*

1. Federal Legislation

There are several existing federal statutes that, while not geared specifically towards protecting the privacy of SNS accounts, can provide certain safeguards for applicants. Some of the more relevant laws include the Stored Communications Act,[86] the Fair Credit Reporting Act,[87] the Americans with Disabilities Act,[88] and Title VII of the Civil Rights Act.[89] In addition, Congress has considered two pieces of legislation that deal directly with the issue: the Social Network Online Protection Act[90] and the Password Protection Act of 2013.[91]

The Stored Communications Act (SCA)[92] is designed to prohibit unauthorized individuals from "obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage."[93] Although the SCA does not explicitly cover information on SNS accounts, some courts have applied it to private messaging services that SNSs provide.[94] The SCA, however, will not protect information on an SNS that is made publicly available—the information must "be restricted in some fashion."[95] Enabling privacy settings to restrict access to certain viewers may be enough to qualify.[96] Moreover, at least one court has found that requiring access to such information as a condition of employment can be coercive, thus vitiating the user's authorization.[97]

---

86. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006 & Supp. IV 2011).

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

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

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

90. Social Networking Online Privacy Act, H.R. 537, 113th Cong. (2013). This bill died upon the expiration of the 113th United States Congress, which had referred it to committee.

91. Password Protection Act of 2013, H.R. 2077, 113th Cong. (2013). Like SNOPA, this bill also died upon the expiration of the 113th Congress.

92. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006 & Supp. IV 2011).

93. *Id.* § 2701(a).

94. *See, e.g.,* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980–82 (C.D. Cal. 2010) ("Recognizing that all three sites provide private messaging or email services, the court is compelled to apply the voluminous case law cited . . . that establishes that such services constitute [electronic communication services].").

95. *Id.* at 981.

96. *See id.* at 981–82.

97. Pietrylo v. Hillstone Restaurant Group, No. 06-5754, 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009). In this case the access to such information was a condition of continued employment; whether it is a condition of initial or continued employment is immaterial, though, as both demonstrate that the employer's willingness to employ the employee turns on whether the employee provides access to her SNS.

The Fair Credit Reporting Act (FCRA)[98] regulates the activity of consumer reporting agencies, which provide "consumer credit, personnel, insurance, and other information."[99] These agencies are required to adopt "reasonable measures" to ensure the "confidentiality, accuracy, relevancy, and proper utilization" of the information they provide.[100] A consumer reporting agency is "any person which . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit or other information on consumers for the purpose of furnishing consumer reports to third parties."[101] The FCRA thus applies to many different kinds of background checks, including those "particularly relevant to the social media pre-employment screening context."[102] But only third-party reports (i.e., those *not* conducted by the prospective employer) fall under the ambit of the FCRA.[103]

Two anti-discrimination regimes, the Americans with Disabilities Act (ADA)[104] and Title VII of the Civil Rights Act (Title VII),[105] might restrict a prospective employer's ability to utilize information contained on an applicant's SNS account. The ADA prohibits employment discrimination on the basis of disability, as long as the applicant "can perform the essential functions of the employment position" either with or without "reasonable accommodation."[106] Under Title VII, employers cannot discriminate against applicants on the basis of race, color, sex, national origin, or religion.[107] An SNS account may contain information relating to the applicant's membership in one of these protected classes, which can create grounds for a discrimination claim if the applicant is not hired. Though Title VII is satisfied if the employer's decision is based on non-discriminatory reasons, requiring the disclosure of protected class status during an interview can be evidence of discrimination.[108] Similarly, the ADA bars any inquiry into "the existence, nature, or severity of a disability"—whether that information is eventually used to make an employment decision is immaterial.[109]

98. Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681t (2006).
99. *Id.* §§ 1681(b).
100. *Id.*
101. *Id.* § 1681a(f).
102. Ebnet, *supra* note 13, at 307.
103. *Id.*
104. Americans with Disabilities Act, 42 U.S.C. §§ 12111–12117 (2006).
105. Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e–2000e-17 (2006).
106. Ebnet, *supra* note 13, at 311.
107. Title VII of the Civil Rights Act of 1964, 42 U.S.C. §§ 2000e–2000e-17 (2006).
108. Ebnet, *supra* note 13, at 311.
109. *Id.*

Thus, a prospective employer may be inviting a lawsuit by demanding access to applicants' SNS accounts.

In addition to these existing protections, the 113th Congress proposed legislation to address the issue of employee and applicant SNS account privacy. The Social Networking Online Protection Act (SNOPA)[110] covers employees and applicants[111] as well as students.[112] The employee/applicant provision of SNOPA is similar to the state laws cited below[113] and prohibits employers from requesting access to an applicant's SNS account or from taking adverse employment action in the event that the applicant refuses to provide such access.[114] The Act would be directly enforceable by the Secretary of Labor, who would be empowered to bring cases in federal district court arising out of SNOPA violations.[115] The proposed Password Protection Act of 2013 (PPA)[116] also speaks to the issue, as it would "prohibit employers from forcing prospective or current employees to provide access to their own private, personal data systems as a condition of employment" while "retain[ing] employers' rights to govern access to [SNSs] within office hours and set policies for employer-operated computer systems and accounts."[117] Both SNOPA and the PPA died in committee, however. The next Section will turn to states' efforts to address this issue with legislation of their own.

2. State Legislation

Perhaps in an effort to inject some clarity into the law, several states have passed laws forbidding the practice entirely. As of January 2014, twelve states have passed laws addressing the employer practice of requesting access to applicants' SNS accounts: Arkansas,[118] California,[119] Colorado,[120] Illinois,[121] Maryland,[122]

110. Social Networking Online Privacy Act, H.R. 537, 113th Cong. (2013).
111. *Id.* § 2.
112. *Id.* §§ 3–4.
113. *See infra* Part II.B.2.
114. H.R. 537 § 2(a).
115. H.R. 537 § 2(b)(2); *see also* Gerano, *supra* note 4, at 679.
116. Password Protection Act of 2013, H.R. 2077, 113th Cong. (2013).
117. Brutocao, *supra* note 34, at 10 (referring to the PPA of 2012, which is virtually identical to the PPA of 2013).
118. ARK. CODE ANN. § 11-2-124 (2013).
119. CAL. LAB. CODE § 980 (West 2014). It is worth noting that both *O'Connor* and *Quon* originated in California.
120. COLO. REV. STAT. § 8-2-127 (2013).
121. 820 ILL. COMP. STAT. 55/10 (2013), *amended by* 2013 Ill. Legis. Serv. 98-501 (West).
122. MD. CODE ANN., LAB. & EMPL. § 3-712 (LexisNexis 2013).

Michigan,[123] Nevada,[124] New Jersey,[125] New Mexico,[126] Oregon,[127] Utah,[128] and Washington.[129] A representative statute reads as follows:

> An employer shall not do any of the following:
>
> (a) Request an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account.
>
> (b) Discharge, discipline, fail to hire, or otherwise penalize an employee or applicant for employment for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account.[130]

These statutes uniformly prohibit employers from requiring applicants to provide access to their personal SNS accounts, and most prohibit the employer from taking any adverse action as a result of an applicant's failure to provide such access. As of January 2014, seventeen other states are considering similar legislation.[131]

Despite the recent state legislation, the state of the law regarding applicant privacy in SNS accounts is unclear. It remains an open question whether SNS users can claim a reasonable expectation of privacy in their accounts, thus leaving applicants vulnerable in both the public and private sectors. Even if users can claim a reasonable expectation of privacy in their accounts, it is also unclear whether requesting access to an applicant's SNS account would be unreasonable or highly offensive to a reasonable person. Some existing federal legislation may or may not be applicable to the practice, and Congress is having trouble passing its own laws that specifically prohibit employers from making these demands. Furthermore, the

---

123. MICH. COMP. LAWS § 37.273 (LexisNexis 2012).

124. Assemb. 181, 2013 Leg. 77th Sess. (Nev. 2013), *available at* http://www.leg.state.nv.us/Session/77th2013/Bills/AB/AB181_EN.pdf.

125. N.J. STAT. ANN. §34:6B-6 (West 2013).

126. N.M. STAT. ANN. § 50-4-34 (2013).

127. H.B. 2654, 77th Gen. Assemb., Reg. Sess. (Or. 2013), *available at* https://olis.leg.state.or.us/liz/2013R1/Measures/Text/HB2654/Enrolled.

128. UTAH CODE ANN. § 34-48-201 (LexisNexis 2013).

129. WASH. REV. CODE § 49.44.200 (West 2013).

130. MICH. COMP. LAWS § 37.273 (West 2013).

131. *See Employer Access to Social Media Usernames and Passwords*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 7, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014.

proposed federal laws, like the state legislation, frustrate the legitimate interest of employers. From all this uncertainty arises an imperative to clarify the law and add some stability to the issue. Part III will offer a means to accomplish that objective: a modified information escrow that both protects the substance of applicants' SNS accounts and provides employers with information relevant to the hiring decision.

III. THE WAY FORWARD: AN INFORMATION ESCROW TO ACCOMMODATE THE NEEDS OF APPLICANTS *AND* EMPLOYERS

A. The Inadequacy of Privacy Law and Proposed Solutions

The methods of addressing the question of SNS privacy for applicants can be divided into three basic categories: (1) existing privacy law (constitutional, statutory, and common law); (2) the passage of new legislation (both at the state level and at the federal level); and (3) repurposing existing federal legislation to accommodate the practice at issue. None of these approaches adequately addresses both applicants' desire for privacy and employers' legitimate need for relevant information. Privacy law as it stands now is too vague with regard to the privacy of an employee's SNS account, and even where there are concrete standards, they tend to be highly unfavorable to the employee.[132] State laws, meanwhile, fail entirely to account for the employers' needs by forbidding them from requesting access to applicants' SNS accounts in any form. The proposed federal legislation suffers from the same malady. Finally, the repurposing of existing federal laws will either require entirely new legislation, a solution that will suffer from the sluggishness of the federal legislative process, or leave undesirable gaps in coverage.

The discussion above demonstrates the muddled nature of privacy law as applied to SNS accounts.[133] Courts have not even been able to agree whether an applicant has a reasonable expectation of privacy in an SNS account, the prerequisite to asserting any right against a potential employer. If anything, the current trend seems to be against finding a reasonable expectation of privacy,[134] leaving applicants at the mercy of the job market and their potential employers. Compounding the problem is the fact that existing privacy

132. *See supra* notes 68–71 and accompanying text.
133. *See supra* Part II.A.
134. *See* Feuer, *supra* note 11, at 492–95.

law pertains primarily to physical spaces, such as an office.[135] As a result, it is ill-equipped to deal with privacy problems online and has not translated well into that context.[136] Even if courts were to find that applicants have reasonable expectations of privacy in their SNS accounts, the current decisions in privacy law afford no middle ground between employee privacy interests and employer interests in learning important information about applicants. Privacy law does not appropriately accommodate the interests at stake.

Legislation on the subject has also proved incapable of effectively addressing the problem. State laws passed to date simply bar employers from requesting access to applicants' SNS accounts, period.[137] The proposed federal legislation on the topic (SNOPA and PPA) would also accomplish largely the same objective.[138] The proposed federal laws, however, have struggled to gain traction in Congress and failed to pass.[139] Laws like these are certainly effective means for protecting applicants' privacy, but they do not account for the legitimate needs of employers. The information contained on applicants' SNS accounts is highly useful in screening out undesirable candidates (and especially those who may become liabilities).[140] Stripping employers of any access to this relevant information should only be done if there are no other means of adequately protecting applicants' privacy.

Proposals for repurposing existing federal legislation attempt to strike a balance between applicant privacy and employer interests. The laws that these proposals utilize, however, are currently insufficient to reconcile those competing concerns. The SCA has proved difficult to apply in the social media context, and the courts that have found it applicable to information contained on SNS accounts have only been able to do so via " 'legal acrobatics.' "[141] In fact,

---

135. *See, e.g.*, O'Connor, 480 U.S. at 715–19; *see also* Del Riego et al., *supra* note 25, at 18 ("In the United States, privacy law has largely been formulated around the physical realm . . . .").

136. Del Riego et al., *supra* note 25, at 18; *see also* Ghoshray, *supra* note 33, at 556 ("[E]nhanced functionalities within cyberspace have reconfigured the way individuals interact online . . . yet the legal protection for such private communications has not evolved accordingly.").

137. *See supra* Part II.B.2.

138. *See supra* Part II.B.1; *see also supra* text accompanying notes 110, 115–17.

139. *H.R. 537: Social Networking Online Protection Act*, GOVTRACK.US, https://www.govtrack.us/congress/bills/113/hr537 (last visited Jan. 6, 2015); *H.R. 2077: Password Protection Act of 2013*, GOVTRACK.US, https://www.govtrack.us/congress/bills/113/hr2077 (last visited Jan. 6, 2015). Additionally, the Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012), died in committee. *H.R. 5684 (112th): Password Protection Act of 2012*, GOVTRACK.US, https://www.govtrack.us/congress/bills/112/hr5684 (last visited Jan. 28, 2014).

140. *See supra* text accompanying notes 23–25, 27–29.

141. Feuer, *supra* note 11, at 499 (citation omitted).

advocates for the SCA as a solution to the problem of applicant SNS privacy acknowledge its inability to adapt to social media, choosing instead to focus on reforming the law rather than applying it in its current form.[142] The SCA will remain "outdated and difficult to apply to modern technology"[143] until it is amended, a process that, based on the current treatment of SNOPA and PPA, will be slow and, in all likelihood, unfruitful.[144]

The FCRA's major limitation is that it only applies to searches conducted by third parties, meaning that employers who conduct pre-screening in-house are exempt from its restrictions.[145] Consequently, for the FCRA to serve as a meaningful limitation on employers' ability to search applicants' SNS accounts, third-party searches must be mandatory.[146] Furthermore, even if the law required that third parties conduct searches of applicants' SNS accounts, the FCRA does not limit the information to which the third party and, consequently, the employer, may gain access. Rather, the FCRA requires only that the employer obtain the applicant's consent prior to conducting the search[147] and notify the applicant if adverse action is taken as a result of the search.[148] As long as those requirements are met, the third party has access to whatever information is publicly available (including substantive content from the applicant's SNS account) and can transmit that information to the employer. At the same time, the FCRA does not, by itself, authorize access to that information on an SNS account that the applicant has protected from public view. The search is thus both overly invasive—in that the employer can gain access to any of the applicant's available substantive SNS content—and insufficiently informative—in that it does not enable the examination of all potentially pertinent information contained on an SNS account. In other words, the employer has access to information other than that which is necessary to effectively pre-screen an applicant, but not to all the information likely to be relevant. Hence, the FCRA is an inadequate solution to the problem.

Title VII and the ADA are also insufficient to address the issue. These statutes forbid employers from gaining access to information

142. *See id.* at 499–503; *see also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("[T]he existing statutory framework [of the SCA] is ill-suited to address modern forms of communication . . . .").

143. Feuer, *supra* note 11, at 511.

144. *See supra* note 139 and accompanying text.

145. Ebnet, *supra* note 13, at 314, 328–29.

146. Ebnet, *supra* note 13, at 329.

147. 15 U.S.C. § 1681b(b)(2)(A)(ii) (2012).

148. 15 U.S.C. § 1681m(a)(2)(A)(i).

regarding an applicant's membership in certain protected classes;[149] they do not reach any private information outside of that. As long as an employer's search of an applicant's SNS account does not yield information regarding such membership, neither Title VII nor the ADA would pose a barrier. Consequently, these statutes do not sufficiently protect applicants' privacy. On the other hand, employers considering a search of an applicant's SNS account can never be sure whether the account will reveal information regarding the applicant's membership in a protected class. In an effort to avoid potential discrimination lawsuits, an employer may choose to forego any review of the applicants' SNS accounts. As a result, Title VII and the ADA also do not appropriately account for employers' needs in pre-screening applicants. Instead, a different approach is needed, one that maximizes both employers' and applicants' ability to get what they want.

B. The Best of Both Worlds: A Modified Information Escrow

Although the current state of the law does not offer an adequate solution to the problem of applicant SNS privacy, there is a system that will serve the legitimate interests of both applicants and employers. The solution is a modified information escrow that will simultaneously provide employers with the information they need and protect the substance of applicants' SNS accounts[150] from the prying eyes of potential employers.

1. Information Escrows and Adaptation to the Employer/Applicant Context

An information escrow is "a mechanism of conditional, *intermediated* communication" that "allow[s] the user to deposit information into [the] escrow lockbox with instructions . . . that the information only be released to prespecified recipients under prespecified circumstances."[151] The escrow necessarily involves a third party (the escrow agent), but seeks to limit or eliminate third-party discretion

149. *See supra* text accompanying notes 104–09.

150. By "the substance of applicants' SNS accounts," "substantive content of SNS accounts," and similar phrases, I mean the content located on such accounts that forms the basis for the conclusions employers seek to draw about the applicant. Such content includes photos, wall posts, status updates, tweets, and the like.

151. Ian Ayres & Cait Unkovic, *Information Escrows*, 111 MICH. L. REV. 145, 150 (2012).

via the limiting conditions placed upon the release of the information.[152] Some common forms of information escrows are commitment escrows, into which the depositor places "embarrassing or incriminating information that will be released if the depositor fails to keep a commitment,"[153] and posthumous escrows, from which deposited information is released after a predetermined period of time following the depositor's death.[154] Interestingly, the two examples just cited serve contrary purposes: the depositor for a commitment escrow hopes that the information deposited will *not* be released, instead using the threat of release as an incentive to adhere to a certain course of action in a form of self-imposed blackmail; the depositor for a posthumous escrow, on the other hand, is ensuring that the information eventually *will* be released.[155] Information escrows are thus capable of adaptation to serve different ends. This flexibility gives these escrows a leg up over the rigid mechanisms mentioned previously.[156]

The information escrow for potential employees would require the applicant to "deposit" her SNS account password(s) with the "escrow agent," a third party acting on behalf of the employer, who would then search the SNS account for information relevant to the employer's hiring decision.[157] In its traditional form as described above, the information escrow would do little to assist in this process. If the depositor (in this case, the applicant) could set the conditions of the release of information, then it is unlikely that the employer would ever receive any information at all, let alone any useful information. Consequently, in this context it would be the employer setting the conditions of release via a list of "red flags" provided to the escrow agent. On this list would be activities and information that the employer considers relevant to the hiring decision (e.g., drinking, drug use, and negative comments regarding

152. *Id.*
153. *Id.* at 151.
154. *Id.* at 153.
155. *Id.*
156. *See supra* Part III.A.
157. This is the method by which the information escrow would have to operate at the present time. A far more convenient method would involve the SNS itself providing a function that would enable the escrow agent to view the private information without the applicant having to provide her password. For example, an SNS could create a user category for escrow agents such that, utilizing proper authentication procedures, the escrow agent would simply be granted access to the private parts of the applicant's SNS account without the cumbersome intermediate step of providing the escrow agent with a password and its accompanying difficulties (addressed more fully in Part III.B.2, *infra*). Legislatures cannot mandate that SNSs provide such an option, which is why the proposed escrow is structured the way it is. If this approach is adopted, however, perhaps the SNSs would create the escrow agent functionality on their own.

employers). If, in the course of the search, the escrow agent discovers any of these red flags, the agent will indicate the presence of that information, for instance by checking a box next to the appropriate red flag on the list of relevant hiring criteria. Once the search is completed, the escrow agent then returns the red flag list to the employer.

This modified information escrow recalibrates the budget of available information, so to speak, between the applicant's privacy interest and the employer's interest in relevant information because it provides the employer with all (or most) of the information she needs to make an educated hiring decision while simultaneously protecting the substance of the applicant's SNS account from the employer's prying eyes. To illustrate this point, imagine that the achievement of each actor's goal[158] is measured on a scale of zero (not at all achieved) to one hundred (completely achieved). In a state that bans the practice of requesting access to an applicant's SNS account, the applicant keeps all of his SNS information private (one hundred) and the employer gets none of the information she wants (zero) for a total of one hundred. By using a modified information escrow, the employee is able to keep virtually all of the substantive content of his SNS account private (say, somewhere between eighty and ninety), and the employer would also have access to nearly all of the information that she wants (also between eighty and ninety) for a total score of somewhere north of 160.[159] In this way, the information escrow does not *balance* the interests of the two parties so much as it *expands* the available framework within which to operate.

This result can be analogized to the system of credit reporting. Based on an applicant's "bill-paying history, including late collection actions," credit reporting agencies provide employers with a credit score reflecting that history.[160] As a result, the employer receives the information relevant to the hiring decision (e.g., that the applicant has, for the most part, handled her finances well) without learning the private details (e.g., that the applicant did not pay a few credit card bills on time) that form the basis of that information. In the same way, the modified information escrow would

158. The applicant's goal is to keep as much private information private as possible, while the employer's goal is to obtain as much information relevant to the hiring decision as possible.

159. These figures are, of course, speculative. The budget of available information will be successfully recalibrated, however, as long as each actor achieves better than half of his goal (i.e., better than a score of fifty)—because the total score of a ban will always be one hundred, any score above that improves the net outcome of the system.

160. Ebnet, *supra* note 13, at 312–13.

provide employers with pertinent information (e.g., that the applicant drinks socially) without seeing the source of the information (e.g., that embarrassing picture of the applicant chugging a beer during spring break in college) that the applicant would prefer to keep private.

While the modified information escrow would do much to protect an applicant's privacy, it necessarily does less than an outright ban. This means that some measure of applicant privacy will be sacrificed to the gain of employers. Applicants will likely be unhappy with this solution, since they will be less protected. But unlike the existing state bans and the proposed federal bans on the practice of requesting SNS account access, this solution has the advantage of acknowledging that there are two relevant actors engaged in this transaction (the applicant *and* the employer) and that each has legitimate interests at stake. So, while it is true that this solution does not work out as well for applicants, the marginal loss to their privacy is more than offset by the tremendous gain for employers, whose needs should also be taken into account.

In addition to the recalibration of the informational budget, this system would prevent the employer from gaining access to potentially controversial information that should not have any bearing on the hiring decision. For example, perhaps an applicant enjoys a particular singer or genre of music that the employer finds offensive and the applicant discloses that interest on her SNS account. If the employer were to view the applicant's SNS account directly or otherwise gain access to its substantive content, that information may, consciously or unconsciously, influence the employer's ultimate decision. Using the modified information escrow, on the other hand, the employer would never access that information and as a result, could not hold it against the applicant.

Another benefit of using a modified information escrow to conduct searches of applicants' SNS accounts is that, because the escrow agent is a third party, the FCRA would apply. Hence, the information escrow would achieve all the protection offered by the FCRA in addition to its own inherent safeguards. As mentioned above, the FCRA mandates that the applicant give consent to the search and also that the applicant be notified if the search results in a negative hiring decision.[161] This latter requirement is especially important in this context because it would be valuable evidence in a potential lawsuit to enforce an applicant's rights under a contract

161. *See supra* text accompanying notes 147–48.

creating the information escrow or to recover damages for a breach thereof.[162]

2. Avoiding Abuses and Answering Objections

Although the use of modified information escrows is a promising solution, it is not perfect—the potential for abuse would require additional regulation. The applicant, employer, and escrow agent can all subvert the system, thereby destroying the advantages that these information escrows are designed to secure. Additionally, there are several objections that might be leveled at the use of this system. While not exhaustive, this Section attempts to address at least the major abuses and objections that accompany the proposal.

The most obvious means to address potential abuses is to require that the information escrow be created by a contract between the applicant, the employer, and the escrow agent. This contract would delineate the rights and responsibilities of each party and provide a cause of action if any party breached an obligation. A comprehensive contract would effectively protect against most of the potential abuses to which these information escrows might be vulnerable. Such a contract would also be cost-effective: once standardized, it could be reproduced and used for all applications.

Applicants will be tempted to conceal as much of their personal information as possible. An applicant might lie and say that she does not have an SNS account, or she may have multiple SNS accounts, only one of which she discloses to the employer. This particular kind of abuse is difficult to address because it is not clear how the employer would discover that the applicant has not been truthful. A partial solution would be to include in the contract an obligation, owed by the applicant to the employer, to provide the escrow agent with passwords to all of the applicant's personal SNS accounts. The clause should also indicate that the applicant's failure to abide by this requirement would, if the applicant is hired, constitute grounds for termination once discovered. This would provide a strong incentive for a serious applicant to be forthcoming regarding her SNS accounts.

Employers, on the other hand, may try to use their control over the escrow conditions to obtain information that goes beyond the scope of a reasonable search. Some criteria, such as drug use, would likely be universally accepted as relevant to the hiring decision, just as other criteria, like taste in music, would generally be considered

162. *See infra* Part III.B.2.

irrelevant. Between those extremes, however, is where the difficulty lies. Because different employers value different characteristics, what might be a red flag for one employer would not necessarily offend another. A standardized list of criteria would thus be of little utility, meaning that employers would be free to craft their own lists. The lack of a definitive list of criteria against which to measure would, to an extent, leave applicants vulnerable to a particular employer's idiosyncratic views of desirable employee characteristics.

This problem could be mitigated by (1) including in the escrow contract a duty for the employer to request only information regarding criteria that bear a "significant nexus"[163] to a hiring decision and (2) requiring public disclosure of the list of criteria to be used at the time that the job is posted (and an obligation to provide the same list to each applicant prior to the creation of the escrow). The first requirement would both limit the employer's ability to request information and allow for some flexibility by permitting employers to decide what information is important for applicants in their business or industry. The "significant nexus" standard[164] is well-suited to this inquiry—it is less deferential than a "reasonably relevant" standard,[165] but more flexible than an "essential" standard.[166] The second requirement would serve two functions. First, it would give the applicant notice of the information sought from her SNS account, thereby allowing the applicant to either provide informed consent or refuse and withdraw her application. Second, it would act as a check on the employer's impulse to search for extraneous information because the employer would have to either disclose her interest in such information, which would disincentivize application, or operate outside the bounds of the list provided, which would breach the escrow contract.

---

163. Rapanos v. United States, 547 U.S. 715, 759 (2006) (Kennedy, J., concurring) (discussing a "significant nexus" test in the context of the Clean Water Act).

164. Admittedly, the "significant nexus" test originated in the context of the Clean Water Act, but its reasoning can be easily adapted: in the same way that wetlands possess a significant nexus with navigable waters because they are " 'integral parts of the aquatic environment,' " *id.* at 779, employers' criteria will bear a significant nexus to the hiring decision if they are "integral" thereto. There will also have to be a reasonableness component to the inquiry to ensure that employers cannot utilize irrelevant criteria simply because such criteria are, from the *employer's* perspective, integral to the hiring decision. A requirement that the criteria be objectively reasonable should alleviate this concern.

165. *See* F.T.C. v. Carter, 636 F.2d 781, 788 (D.C. Cir. 1980) (finding that the "reasonably relevant" standard is satisfied so long as the information sought is " 'not plainly irrelevant' " to the purpose motivating the search).

166. *See* Hoskins v. Oakland County Sheriff's Dept., 227 F.3d 719, 726 (6th Cir. 2000) (defining "essential function" as a "fundamental" duty of the employment position).

The primary concern with regard to the escrow agent would be the appropriate use of the information to which the agent is given access. As an initial matter, requiring applicants to disclose their passwords constitutes a security risk because many people use the same password for different things, such as email and online banking.[167] To avoid this risk, the agent should instruct the applicant to change her password to one assigned by the agent prior to the search. This will enable the agent to access the account temporarily and once the search is completed, the applicant can return to her original password.[168] Another potential abuse is the risk of the escrow agent using information obtained as a result of the search for personal gain. This issue could be addressed by a clause in the escrow contract forbidding such action. Finally, the escrow contract would also have to include a duty of confidentiality that prohibits the agent from disclosing the information contained on the account to anyone other than the employer. That duty should also prohibit the agent from disclosing more information than necessary to complete the red flag list. Utilizing hiring standards for escrow agents similar to those of credit reporting agencies may also alleviate confidentiality concerns.

In addition to the possible abuses described above, this solution is subject to other criticisms. Perhaps the most significant objection is the potential cost of implementing such a system. There are three major components in assessing this cost: (1) the requisite changes in the law; (2) the creation of escrow agencies to conduct the searches; and (3) the cost of the searches to employers. Implementing the escrows in states that have banned employer SNS searches will require a change in the law. While a full repeal of the law would permit the use of modified escrows, the ideal solution is to create an exception to the ban allowing their use. The benefit of this exception is that the escrows would be the only means for employers to carry out these searches, thereby guaranteeing that employers would either use them and gain the attendant benefits or be unable to conduct any such searches at all. The political cost of such an amendment would be less than a full repeal because the exception

---

167. *See* Carrie-Ann Skinner, *One-Third Use a Single Password for Everything*, PCWORLD (Mar. 11, 2009, 11:10 AM), http://www.pcworld.com/article/161078/one_third_use_same_password.html (reporting that approximately thirty-three percent of Internet users utilize the same password for multiple online applications).

168. The risks of the escrow agent misusing the applicant's password or of the password otherwise being exposed to non-authorized users only exists in a system that requires the applicant's password to gain access to the private content of the applicant's SNS account. If there were an alternative means for the escrow agent to access that content, the need for this elaborate system would be obviated. *See, e.g.*, *supra* note 157.

would be narrow and it would benefit employers while minimizing the intrusion on applicants' privacy. Consequently, any loss of political support from those applicants adversely affected should be offset, at least to some extent, by a corresponding increase in goodwill from employers.

The second cost component is the creation of an entirely new industry of SNS escrow agents to conduct these searches. This obstacle, however, is less daunting than it initially appears. For one thing, there are already agencies that perform similar kinds of work,[169] meaning that hopeful SNS escrow agents would not have to reinvent the wheel, so to speak. Furthermore, there is minimal expertise required to conduct a search of an SNS profile, so recruiting escrow agents should not pose much difficulty, and there will be virtually no training costs. As long as there is a demand for the modified escrows, there will be an incentive for companies to enter the market to provide the service.

Implementing the escrow system will also impose additional costs on employers. One of the major benefits of SNS research for employers is that it can be conducted in-house for little to no cost;[170] requiring that employers outsource the work eliminates that incentive. But denying employers the ability to conduct any form of SNS search also imposes a cost by precluding the most informed possible hiring decision. Amending the ban on employer SNS searches to exempt modified escrows would allow employers to engage in a cost-benefit analysis to determine whether to utilize an escrow in the hiring process. The cost would thus be imposed only on those willing to bear it, and it would likely be offset by the benefit obtained by those employers who choose to incur it.

Though the actual cost per applicant of the escrow system is necessarily speculative at this point, it seems unlikely that it would be prohibitively expensive. Some background checks are indeed costly—for example, a Secret-level security clearance check runs between $210 and $272, while a Top Secret-level check costs almost $4,000.[171] A Secret-level security clearance, however, is a highly intensive process that involves "automated and manual checks of criminal history, terrorist activities, credit, and foreign activities and

169. Some headhunting companies utilize SNS profiles to match the owners of those profiles with employers seeking applicants. *See, e.g.*, *What We Do*, SOCIAL MEDIA SEARCH, http://www.socialmediasearch.co.uk/what-we-do/ (last visited Oct. 8, 2014).

170. *See supra* note 29 and accompanying text.

171. OFFICE OF MGMT. AND BUDGET, SUITABILITY AND SECURITY PROCESSES REVIEW REPORT TO THE PRESIDENT FEBRUARY 2014 3 (2014), *available at* http://fas.org/sgp/othergov/omb/suitsec-2014.pdf.

influence."[172] Where warranted, "additional checks, including interviews and other more manual efforts, are conducted."[173] An SNS search will not involve such herculean efforts and may more readily be compared to a credit report, which costs significantly less.[174] In sum, these escrows will cost employers money, but it is unlikely that the costs will of such a magnitude as to render the system unworkable.

Applicants may object that the information requested is private and should not be considered in making a hiring decision. Though the information is not public in the sense that anyone can access it, the information is at least partially public because it is exposed to a portion of the public (i.e., those people to whom the applicant has granted access). The applicant has thus assumed the risk that the permitted viewers might disclose that information. In an individual capacity, the applicant may be willing to accept this risk. If the applicant is hired, however, she becomes a representative of her employer. At that point, the "private" information on the applicant's SNS account would no longer implicate only her, but would also reflect on the employer if one of those permitted viewers disclosed that information. It is fair for an employer to know whether her representatives (i.e., employees) are disseminating improper information on the Internet. Depriving the employer of access to this information would allow the applicant to decide for the employer what risks the employer should assume.

The next objection, from the employers, is that the information escrow approach will be limited by the pre-selected criteria and thus not account for "I know it when I see it"[175] types of information. This objection might refer to either of two kinds of information: ambiguous information that may or may not be a red flag, or information whose relevance to the hiring process does not occur to the employer unless she is presented with it. The first category deals with discretion—when faced with ambiguous information, either the employer or the escrow agent will have to make a judgment call. Allowing the employer to instruct the escrow agent to either disclose or not when confronted with such information would likely resolve this issue in most cases. The second category seems analogous to the idiosyncratic preferences, such as

---

172. *Id.* at 2.

173. *Id.*

174. *See, e.g.*, *Employment Credit Report*, PROFORMA SCREENING SOLUTIONS, http://www.proformascreening.com/employment-screening/personal-identity/ (last visited July 8, 2014) (charging $8.50 for an employment credit report).

175. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (describing "I know it when I see it" in the context of obscenity law).

an applicant's taste in music, that are of questionable relevance in the hiring process. If the criterion is truly pertinent, then it will probably come to the employer's attention at some point, at which time the employer can amend the red flag list for future use. If the omitted criterion never comes to the employer's attention, then it likely does not have a significant nexus to the hiring process. Either way, simple experience using the information escrow over time should resolve this objection.

CONCLUSION

The explosion of social media use has in many ways redefined the ways in which we communicate. SNSs can help people stay in touch with one another and can serve as creative outlets for individual expression and community sharing. But the widespread use of SNSs has also created problems, among them the issue addressed in this Note: how to handle employers' desire to use the information that applicants post online to make hiring decisions. On the one hand, applicants are justified in their reticence to expose private information to people with whom they would prefer not to share it. On the other hand, employers are equally justified in trying to acquire as much relevant information about an applicant as they can to ensure the most informed hiring decision possible. The current legal framework addressing this issue fails to solve the dilemmas because it does not sufficiently account for both parties' legitimate interests.

This Note puts forth a solution that accommodates both applicants' desire for privacy and employers' need for information in a way that would maximize the system's net output, measured by the parties' respective values on privacy and access to relevant information. A modified information escrow protects applicants' privacy interests in the substantive content of their SNS accounts while at the same time providing to employers the information from those accounts that is relevant to the hiring decision—and *only* that information. While this solution may not be ideal for either party, it is a necessary compromise.