UNIVERSITY OF MICHIGAN

JOURNAL *of* LAW REFORM ONLINE

COMMENT

THE NEED TO PREVENT EMPLOYERS FROM ACCESSING PRIVATE SOCIAL NETWORK PROFILES

Brett Novick*

In March 2012, social network privacy became a conversation topic after news reports of the story of Justin Bassett, a job applicant who withdrew his application in the middle of an interview when the interviewer asked him for the username and password of his private Facebook account.[1] Although the issue has received much attention from the public and media, the Department of Justice (DOJ) has stated that it has no interest in prosecuting employers for asking for social networking account information.[2] Fortunately, legislation that would make it illegal for employers to ask for the username and passwords for social networking sites as a condition of hiring a candidate is currently being considered at the state and federal levels.[3] While this is a necessary reform, legislatures should go one step further and truly protect private social networking by preventing employers from accessing these accounts through other methods.

I. THE IMPORTANCE OF PROTECTING PRIVATE SOCIAL NETWORKING INFORMATION

Employers argue that they want access to a candidate's private social networking profile as an additional method of assessing the background of the applicant, and to make sure that candidates are ethical people and behave in such a way that does not contradict

* J.D. Candidate, May 2014, University of Michigan Law School.

1. *See* Manuel Valdes & Shannon McFarland, *Job Seekers Getting Asked for Facebook Passwords*, YAHOO! NEWS (Mar. 20, 2012), http://news.yahoo.com/job-seekers-getting-asked-facebook-passwords-071251682.html.

2. *Id.* The DOJ regards entering a social networking website in violation of a website's terms of service (TOS) as a federal crime. In Bassett's case, Facebook's TOS prohibited divulging login information to a third party. Thus, an employer using Bassett's login information to access his Facebook's account would be committing a federal crime. *See id.*

3. *See infra* notes 15-20 and accompanying text.

the core values of the company.[4] Accessing a candidate's social networking profile is one tool an employer has to determine whether the candidate is of good character. For example, the employer can make sure that there are no references to illegal drug use or other explicit material on the candidate's Facebook page.[5] Further, since the process takes only a few minutes, it can be seen as a cost-effective means of judging the character of candidates.

This overstepping of social network privacy is a legitimate concern for legislators because (1) it violates the privacy of job candidates; (2) the practice must be deterred to prevent its growth; and (3) it is the wrong move from a business perspective. Courts generally have given a person's private e-mail account similar privacy protection under the Fourth Amendment as that extended to other traditional forms of communication.[6] Similarly, a public entity that demands social network account information from a job candidate to view the candidate's private communications can be seen as breaching the candidate's Fourth Amendment privacy rights.[7] Legislators should thus be concerned about protecting job candidates from similar actions by private firms. Employers might also discriminate in hiring by using information that a candidate wants to keep private and about which the employer could only become aware by looking at a private Facebook profile, such as a candidate's religion or sexual orientation.[8]

---

4. *See* Robert Sprague, *Invasion of the Social Networks: Blurring the Line Between Personal Life and Employment Relationship*, 50 U. LOUISVILLE L. REV. 1, 4–5 (2011).

5. *See* Dan Schawbel, *How Recruiters Use Social Networks to Make Hiring Decisions Now*, TIME MONEYLAND (July 9, 2012), http://moneyland.time.com/2012/07/09/how-recruiters-use-social-networks-to-make-hiring-decisions-now/ (citing a 2012 survey that 78 percent of employers negatively view "references to illicit drugs" on a candidate's social networking profile).

6. *See* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007) ("The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail.").

7. *See* R.S. *ex rel.* S.S. v. Minnewaska Area Sch. Dist. No. 2149, Civ. No. 12–588 (MJD/LIB), 2012WL 3870868, at *12 (D. Minn. Sept. 6, 2012) (denying defendants' motion to dismiss a Fourth Amendment claim when defendants threatened plaintiff student into revealing her Facebook password in order to gain access to her private information and messages, regarding which plaintiff has a reasonable expectation of privacy).

8. *See* Kathleen Elliot Vinson, *The Blurred Boundaries of Social Networking in the Legal Field: Just "Face" It*, 41 U. MEM. L. REV. 355, 390 (2010) (referring to the risk of a discrimination lawsuit if an employer screens candidates based on information gathered

Unless legislators act now, even more employers will ask for social networking account information from candidates. A 2010 survey revealed that 80 percent of recruiting professionals admitted to researching applicants online, with 63 percent using social networking sites.[9] These percentages are increasing: in a 2012 survey of over one thousand companies, 92 percent indicated that they use social networking for recruiting, and 73 percent research a candidate's social networking profile.[10] Given the current state of the economy, many employers have significant leverage in job interviews. Companies thus can get away with asking for social network account information to gain access to the private accounts of candidates. The current market imbalance might be a factor in causing employers to invade the privacy of candidates; but when the economy recovers, employers will possibly continue to request account information because of the growth of social networking.

Finally, the government should take interest in this practice, as it might have an adverse effect on businesses.[11] As evidenced by Bassett's reaction, potential candidates might refuse to divulge their account information on principle.[12] An employer could further harm itself if the practice is revealed and causes a public relations issue for the company.[13] And companies are better off taking advantage of employees' social media connections to reach

---

from a social networking site). Likewise, an employer's access to an employee's social network information may expose the employer to liability after a hiring decision is made. For instance, an employee could attempt to tie an adverse employment decision to a supervisor's prior "friend" request, alleging that "protected category" information contained in the employee's Facebook profile page unlawfully influenced the employer's decision. *See* Maureen Minehan, *Should Supervisors and Employees be "Friends?"*, 19 INT'L HR J., no. 2, Spring 2010.

9. Sprague, *supra* note 4, at 4–5 (citing CROSS-TAB, *Online Reputation in a Connected World* 8 (Jan. 2010), http://go.microsoft.com/?linkid=9709510).

10. Schawbel, *supra* note 5.

11. Jeanne Meister, *Facebook and the Job Interview: What Employers Should be Doing*, FORBES (Apr. 9, 2012, 12:34 p.m.), http://www.forbes.com/sites/jeannemeister/2012/04/09/facebook-and-the-job-interview-what-employers-should-be-doing/.

12. *See id.* (quoting a twenty-six-year-old employee who said that a prospective employer asking him for his social networking password "would be a total non-starter").

13. *See id.*

out to their contacts,[14] rather than chilling their use of social networking by adopting a "big brother" mentality.

II. PROPOSED LEGISLATION HELPS TO PROTECT SOCIAL NETWORK PRIVACY

Given DOJ's unwillingness to prosecute TOS violations and the reasons set forth above, it is necessary to pass legislation that makes it a crime for employers to ask for social network account information. In May 2012, Maryland became the first state to bar an employer from requesting or requiring account information from social networking sites as a condition of employment.[15] Illinois passed a similar law in August 2012,[16] and California Governor Jerry Brown signed privacy legislation shortly thereafter, on September 27, 2012.[17] Many other state legislatures have introduced similar legislation, although they have not been as quick to pass these laws.[18] Meanwhile, U.S. Representative Elliot Engel (D-NY-17) introduced the Social Networking Online Protection Act last April, which would make it unlawful for an employer to request account information for a personal account on a social networking website.[19] The bill would also authorize the U.S. Secretary of Labor to institute civil penalties of up to $10,000 against employers who violate the Act.[20] But the bill has had little traction thus far.

In passing such legislation, states can use their police power to ensure that companies do not infringe on the privacy of

---

14. *See id.* (referring to PepsiCo's plans to use employees' social media and Facebook accounts to market the company to their friends and provide more exposure).

15. Act of May 2, 2012, 2012 MD. LAWS Ch. 233 (effective Oct. 1, 2012) (to be codified at MD. CODE ANN., LAB. & EMPL. § 3–712) (prohibiting an employer from requesting a username or password from an employee or applicant to access a personal account).

16. Right to Privacy in the Workplace Act, 820 ILL. COMP. STAT. 55/10 (West 2012) (effective Jan. 1, 2013) (barring an employer from asking an employee or applicant for account information to access a profile on a social networking website).

17. Act of Sept. 27, 2012, 2012 CAL. LEGIS. SERV. Ch. 618 (to be codified at CAL. LAB. CODE § 980); Sarah Jacobsson Purewal, *California Bars Employers from Demanding Employees' Social Media Log-in Info*, TECHHIVE (Sept. 28, 2012 7:17 AM), http://www.techhive.com/article/2010785/california-bars-employers-from-demanding-employees-social-media-log-in-info.html.

18. *See, e.g.*, H.B. 308, 146th Gen. Assemb., Second Reg. Sess. (Del. 2012); H. File 2963, 87th Legis. Sess., Second Reg. Sess. (Minn. 2012); S.B. 1915, 215th Leg., First Ann. Sess. (N.J. 2012); H.B. 2332, 196th Gen. Assemb. (Pa. 2012).

19. Social Networking Online Protection Act, H.R. 5050, 112th Cong. (2012).

20. *Id.*

citizens.[21] Some have suggested that existing federal law, such as the Stored Communications Act (SCA), may already protect social networking privacy.[22] But new legislation will more effectively regulate employers by providing candidates with specific laws designed to protect social network account information and information posted on private social networking profiles, rather than relying on existing federal legislation whose scope is uncertain.[23] And given that federal legislation was proposed, some members of Congress either do not believe that the SCA provides adequate protection or believe that additional safeguards are required.[24]

III. SEPARATING PRIVATE SOCIAL NETWORKING AND THE WORKPLACE

While the newly enacted statutes are a step in the right direction, legislators should take further action to prevent employers from using other methods to access private social networking accounts. For instance, employers can access a candidate's private social networking account by coercing a third party who is a friend of the candidate to give them the third party's own account information in order to see the candidate's profile.[25] Currently proposed legislation would prohibit this

---

21. *See* State Dep't of Roads v. Popco, Inc., 247 Neb. 440, 442 (1995) (quoting State v. Two IGT Video Poker Games, 237 Neb. 145, 149 (1991)) ("When a fundamental right or suspect classification is not involved in legislation, the legislative act is a valid exercise of the police power if the act is rationally related to a legitimate governmental purpose.").

22. *See* Sprague, *supra* note 4, at 18 ("One could argue that coercing a job candidate to reveal personal information that is otherwise restricted in exchange for being considered for a job would not be an authorized nor freely-given disclosure and, hence, a possible violation of the SCA.").

23. *Cf.* Crispin v. Christian Audiger, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (citing 18 U.S.C. § 2511(2)(g)) (quashing a subpoena under the SCA for private Facebook and MySpace messages since they are inherently private, while remanding the motion to quash subpoena with respect to Facebook wall postings and MySpace comments in order to determine if they are covered under the SCA based off of plaintiff's privacy settings).

24. *See also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (noting that the Electronic Communications Privacy Act (ECPA) "was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results." The SCA is Title II of the ECPA.).

25. *See* Ehling v. Monmouth-Ocean Hosp. Serv. Corp., Civ. No. 2:11–cv–03305 (WJM), 2012 WL1949668, at *5 (D.N.J. May 30, 2012) (denying in part a motion to dismiss when the

specific activity since it involves asking for account information; however, legislation should also cover similar situations in which an employer uses a third party's account in order to view the candidate's profile without asking for account information.[26] And current employees might willingly allow the employer access to their Facebook account to help screen a candidate if the employees are friends or in the same network as the candidate.[27] This is not illegal under current legislation, but would be covered under legislation banning the use of third party profiles to view private Facebook accounts. Finally, employers can force candidates to become friends with the employer, thereby allowing the employer access to the private social network account without needing any account information, thus bypassing the newly enacted legislation.[28]

---

defendant gained access to the plaintiff's Facebook account by forcing plaintiff's coworker and Facebook friend to access his own Facebook account at work in front of a supervisor).

26. *See* Venkat Balasubramani, *Accessing an Employee's Facebook Posts by "Shoulder Surfing" a Coworker's Page States Privacy Claim—Ehling v. Monmouth Ocean Hosp.*, TECH. & MARKETING L. BLOG (June 4, 2012, 9:00 AM), http://blog.ericgoldman.org/archives/2012/06/accessing_an_em.htm (noting that potential legislation should protect against "shoulder surfing," such as when a third party logs in to his or her own account while an employer watches in the background in order to see the candidate's profile or messages).

27. Facebook's "network" feature generally permits members of the same network to view each other's Facebook profiles, even though the network members are not "friends." Carly Brandenburg notes that some companies hire students from specific schools to gain access to that school's network feature. The employer, through the hired student, can then screen candidates from the same school based on the candidate's now-accessible Facebook profile. *See* Carly Brandenburg, *The Newest Way to Screen Job Applicants: A Social Networker's Nightmare*, 60 FED. COMM. L.J. 597, 602–03 (2008). Federal prosecutors likewise have used the network feature to access previously private Facebook pages. *See* United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012) ("Where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment.").

28. *See* Will Oremus, *Could Your Crummy Klout Score Keep You From Getting a Job?*, SLATE FUTURE TENSE BLOG (Oct. 3, 2012, 12:35 PM), http://www.slate.com/blogs/future_tense/2012/10/03/online_privacy_can_employers_use_klout_scores_facebook_profiles_to_screen_applicants_.html (noting that while California's recently passed law with social network account information helps protect private indiscretion, it "doesn't preclude employers from sending applicants a Facebook friend request, which could serve a similar purpose"); Torie Bosch, *Can Legislation Preventing Employers From Requesting Facebook Passwords Really Protect Privacy?*, SLATE FUTURE TENSE BLOG (Mar. 28, 2012, 4:20PM), http://www.slate.com/blogs/future_tense/2012/03/28/employers_don_t_have_to_request_facebook_passwords_to_invade_applicants_privacy_.html ("Particularly in this economy, applicants desperate for jobs may also feel pressure to accept friend requests from their interviewers. This behavior is more difficult to legislate but nearly as pernicious and invasive.").

To help protect social networking privacy, states should broaden protections for social network accounts. For instance, additional legislation could punish employers for using personal Facebook accounts—either their own or those of other employees—to access the private Facebook accounts of candidates. This legislation would make illegal certain actions discussed above that are not covered by currently proposed or enacted legislation. Moreover, the importance of protecting social network account information extends to current employees; although moral outrage has been focused on the story of Bassett and other job applicants, it is important that laws prevent employers from punishing current employees for withholding this information, which the Maryland, Illinois, and California legislation accomplish. Accordingly, although reform is heading in the right direction, there remains work to be done to ensure that candidates and employees truly enjoy social networking privacy.