Pre-employment Screening on Social Media and Job Recruitment

Shantelle Liu

ABSTRACT

The purpose of this research is to analyze how employers' social media surveillance influences job admissions and how American laws tackle this issue. Despite legal restrictions and applicants' reluctance, increasing numbers of companies require prospective employees to provide their social network sites, login information, or change the privacy setting for employers to conduct social media background check. Therefore, there is a need to collect evidence to demonstrate whether this access to social media invades privacy or enhances career opportunities for applicants. Based on that, this research also analyzes how the current legal framework in the U.S. protects individuals' privacy rights and equality. The results of the research will lay a foundation for further discussion on social media privacy protection and provide legal suggestions for lawmakers.

Key Words: Social Media, Job Recruitment, Surveillance, Online Privacy, Background Check

Introduction

Beginning with the advancement of information technology and Internet penetration, the past ten years have witnessed the booming of social media. According to the current statistical data, the number of active social media users have researched 2.8 billion worldwide (Hutchinson, 2017). That is to say, one third of the population on the planet has at least one social media account. Netizens have been engaging in multiple platforms to build their virtual E-identity, in which what they post represent who they are, what they do, where they come from, and what they have done.

Social media, a digital platform that allows audience to connect, communicate, and interact, has been wildly used since 2007 when Facebook, Twitter, Airbnb, Youtube, and other social media popular today were founded. While traditional media are experiencing recession, social media are playing various roles from networking to microblogging and from news sharing to web

conferences. Its ubiquitousness leaves inevitable marks on individuals' personal life and, of course, professional life.

During the recruitment process, companies increasingly take applicants' social media connections into account, both publicly and underground, attempting to get a more comprehensive image about potential employees. While professionalism in social media could help applicants to stand out in some degrees, pre-employment screening on social media may involve some legal issues, including privacy violation, personal information disclosure, and discrimination and bias. Therefore, further analyzing the effects of social media background check on job admissions is worthwhile.

Pre-employment screening

Pre-employment screening refers to the process of investigating the backgrounds of potential employees in an attempt to verify the accuracy of an applicant's claims. Traditionally, pre-employment screening includes past employment verification, credit history, and criminal history. *Background Screening Trends & Best Practices Report 2015* indicates 65% of employers examine social security or identity checks and 65% of them verify whether candidates are eligible to work in the United States.

Nowadays, considering highly development digital world where companies can capture more information about candidates' personality, professionalism, and personal life, the scope of pre-employment screening expands to social media. According to the Career Builder survey, 63% of employers will not hire someone until they research how they appear on social media. The trend is keeping going among companies around the world.

As the old saying goes, everything has two sides. Social media background check has positive and adverse influence on job seekers. For one thing, social media provides extra information that will

not appear on the resume sometimes to recruiters, which can cause hesitation when recruiters make a decision. Career Builder finds that 48% of employers saw something on social media that caused them not to hire someone. Finding out information like excessive drinking or drug use, provocative photos, negative comments, and so on can leave a bad impression to employers, and thus decrease the admission rate and minimize the potential loss to the company or organization.

However, social media can tip the balance as a social capital and contribute to practitioners' professional growth. When employers discover positive information, such as charitable work, athletic achievement, appearing compassionate, and professional image (CTV News, 2016), they are more likely to bolsters the decision to hire the individual.

Privacy Attitude

The awareness of privacy protection and social media is increasing among social media users. The public gradually is attaching more concerns about restricting self-information disclosure and managing self-reputation online. Madden finds that 58% of social network site users restrict access to their profiles (2012). Specifically, in the working environment, only one-third of employees include their direct supervisor in their online network list. 54% of Millennials maintain an expectation on separation between work and personal life (Levin & Riego, 2012, p.99), even though actively participating in online discussion through digital platforms can contribute to the practitioners' professional growth as a social capital (Gilpin, 2011, p. 232).

Under strong social pressure and peer pressure, netizens have to compromise, exposing their personal information in the virtual network in order to obtain social interaction. Dr. Taddicken from Technische University summarizes this phenomenon as the "Privacy Paradox" theory, in which "the perception of privacy is subject to certain processes of negotiation between the individual need for privacy and the concurrent need for self-disclosure" (2013, p. 265). Dr.

Taddicken points out the social media dilemma where users have to struggle sharing personal information but expect privacy networks. When privacy paradox becomes serious to a social media user, the individual may have a type of anxiety disorder called social phobia. This psychological issue is characterized by a significant amount of fear in one or more social interactions. Nowadays, more and more people are struggling with the balance between social needs and privacy concerns.

The ambiguous boundaries between professional life and personal life have been getting even more blurred, and the overlap is expanding. Current employees as well as job applicants encounter privacy invasion by providing their social network site links or login information in response to requests from employers as a compulsory requirement. Yet, sometimes, recruiters may conduct social media background check secretly without information job seekers before an interview even occurs.

It is also possible that some companies may hire a third-party service provider to conduct pre-employment screening on social media. “I think it is naïve to think that in this day and age, with the technology and self-uploaded content available, that human resources and hiring managers do not check social media sites for information,” said Dave Dickerson, president, founder and CEO of Accurate Background Inc., a background checking provider in Irvine, Calif.

The majority of the public disagree with social media background check. Sarah Gordon, associate director of the Sammons Group, says “see the practice of social media vetting as akin to hiring a private detective to snoop on a candidate or perhaps paying someone to break into their home and rifle through their drawers. It isn't fair, it shouldn't be necessary and, in my view, it's a trend that reputable employers should steer well clear of.”

Laws & Regulations

(1) Online Privacy Protection Act

Beginning in 2012, increasing numbers of states in the United States started to enact laws to protect employees' privacy and prohibit employers from accessing candidates' social media, including asking for login information or associated links and requesting candidates to change their pribacy setting. For example, according to Washington State Legislature (RCW 49.44.200):

- An employer may not:
    - Request, require, or otherwise coerce an employee or applicant to disclose login information for the employee's or applicant's personal social networking account;
    - Request, require, or otherwise coerce an employee or applicant to access his or her personal social networking account in the employer's presence in a manner that enables the employer to observe the contents of the account;
    - Compel or coerce an employee or applicant to add a person, including the employer, to the list of contacts associated with the employee's or applicant's personal social networking account;
    - Request, require, or cause an employee or applicant to alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account; or
    - Take adverse action against an employee or applicant because the employee or applicant refuses to disclose his or her login information, access his or her personal social networking account in the employer's presence, add a person to the list of contacts associated with his or her personal social networking account, or alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account.

Similarly, Illinois, California, Delaware, and another twenty-two states prevent employers from authenticating or accessing a personal online account. A number of additional bills on privacy protection topics were introduced during the following legislative sessions.

In 2016, the Uniform Law Commission adopted the Uniform Employee and Student Online Privacy Protection Act (UESOPPA). This federal act restricts an employer's access to employees' or prospective employees' social media accounts, including disclosing the login information, disclosing the content of the account, or accessing the account in the presence of the employer, and so forth. In addition, it is worth mentioning that UESOPPA gives Attorney General and employee or student the right to bring a civil action against an employer or educational institution for privacy violation. A prevailing the beneficiaries may obtain includes:

- injunctive and other equitable relief;
- a civil penalty of up to $1000for each violation, but not exceeding $100,000 for all violations caused by the same event;
- actual damages;
- costs and reasonable attorney's fees.

(2) Anti-discrimination Law

Besides the specific law targeting on online privacy, prospective employees can also use anti-discrimination law to protect their own rights. Anti-discrimination law means the law on the right of people to be treated equally. The Civil Rights Act of 1964 is a fundamental law that protects American workers to have the equal opportunity on job admission. The law covers discrimination based on "race, color, religion, sex, or ethnic origin."

Moreover, based on the United States Department of Labor, the Age Discrimination in Employment Act (ADEA) and the Americans with Disabilities Act (ADA) prohibits discrimination in employment against individuals over 40 years old and against disable people. However, these anti-discrimination laws just cover companies and organizations' recruitment process. "As with other labor standards, independent contractors generally would not be covered by anti-discrimination laws."

When companies or organizations reject a job seeker based on the facts mentioned above, they will have liability with discrimination. While it is not unlawful to collect personal information from public platforms, using personal information such as race, rage, gender, and so on involves potential legal issue. One of good examples of this point is the case study from the University of Kentucky. In 2011, a UK-born scientist named Martin Gaskell sued the University of Kentucky for discrimination, and eventually got $125,000 out-of-court settlement from the education institute. It is because that the university turned down the job offer after finding some creationist views Martin posted online that was the opposite perspective with the position he was applying. Despite the fact that he fulfilled all the requirements listed on the job description, he was still rejected due to social media screening.

In sum, no matter how employers gain information -- it can from a third-party provider, or it can from social media platforms -- as long as employers use personal information covered by the anti-discrimination law against candidates' capability, employers will have liability with discrimination.

(3) Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) is a U.S. Federal Government legislation enacted to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. This legislation is also applied to job seekers. In summary, under the FCRA, a job candidate has the following major rights:

- You must be told if information in your file has been used against you
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Access to your file is limited.

- Consumer reporting agencies may not report outdated negative information.
- You must give your consent for reports to be provided to employers.
- You may seek damages from violators.

Specifically, if companies or organizations want to collection your information on social media, they should inform you in advance. Only after you consent to disclose your information to potential employers can companies or organizations access your profile.

If a pre-employment social media screening qualifies a background check, then then the company needs to comply with the Fair Credit Reporting Act, gaining authorizations from applicants to proceed with the check. A disclosure agreement needs to be provided to applicants, informing applicants that a social media background check will be performed during the recruitment process. Certainly, applicants can choose to authorize or refuse the disclosure agreement. For employers, this is a wisdom way to reduces exposure to liability.

Nevertheless, Federal Court concludes the FCRA is not applicable to LinkedIn and its "reference search" tool. On April 14, 2015, Magistrate Judge Paul S. Grewal issued an order for LinkedIn Corporation to dismiss a proposed class action indicating that LinkedIn violated the Fair Credit Reporting Act. The court found that "LinkedIn does not function as a consumer reporting agency and that the results generated by its Reference Search tool are not consumer reports." This court decision is a cornerstone in helping to shape the contours of the FCRA and its potential applicability to social media networking and related websites.

Current Problems

(1) Lack of academics

Privacy, as a human right, plays a significant role on personal life and professional life. Previous scholarship analyzes in detail the historical development of social media and discusses social

media users' perception of privacy protection. However, these research studies mainly focus on a self-reporting research method and lacks qualitative methods. Studies critically analyzing the positive and negative effects of social media on careers are rare. In addition, few studies have shed light on how social media access affects prospective employees. Therefore, there is a need to determine whether employers' surveillance of social media influences job admission rates as well as how social media screening influence social media users' behavior.

(2) Vague definition in current legal framework

While state lawmakers have been trying to enact laws to protect people's online privacy and lawyers have been attempting to apply existed legislation to the relevant topics, the current legal framework does not give a clear definition on the keywords related on social media pre-employment screen. For example, the Uniform Employee and Student Online Privacy Protection Act defines "online" as "accessible by means of a computer network or the Internet." This definition does not point out specific sites, thus there is a loophole leaving confusion on which social media sites can be covered by this law.

Similarly, The Fair Credit Reporting Act (FCRA) has the issue on vague definition. Technically, FCRA intends to protect consumers' information and privacy. Job applicants, as consumers of social media, leave a large of footprint on online platforms. However, FCRA concludes that LinkedIn is not a consumer reporting agency. Instead, FCRA alleges that "a consumer reporting agency's primary business purpose must be to gather and evaluate consumer credit information in order to furnish reports on those consumers to third parties for a fee."

(3) Difficulty in finding evidence

Based on the discussion above, it is obvious that pre-employment screening on social media is illegal, but in reality, it is difficult to find the evidence showing a company or an organization sneakily peek candidates' social media account and use the online content against candidates'

capability. If a company hack into a person's social media account to troll for information, it can leave trace to the Internet. However, most of companies conduct social media background check throughout researching candidates on major sites like Google or Facebook.

For job applicants, it is hard to obtain recruiters' online search history. Although applicants can use file Freedom of Information Act to request companies to give the reason why they do not get in the position, proving that social media screening is the main reason to reject candidates is a not easy job. Considering employers may use other reasons to explain the rejection, applications actually stand in a disadvantage position in the courtroom.

Potential Solutions

In the digital environment, privacy violation, like information collection and dissemination is increasingly frequent due to the weak legal framework and blurred definition of social media. Here are couple of suggestions future lawmakers can take into account.

(1) Technology

The advancement of technology creates social media that allows companies to harvest and monetize user data, which, in return, can also creates tools for us to protect our online privacy. Currently, there are plenty of internet service providers to help the public add an additional layer of privacy, protection, and security. For instance, I2P, a free open source for secure communication, uses end-to-end encryption to hide the content of your communications, thus others cannot track your behavior and destination. In the near feature, technology may develop new tools specifically for job seekers. Ideally, when an IP address from a potential employer looks through an applicant's social media site, the applicant can receive an alarm and the social media site will automatically change the privacy setting.

(2) Clarify definition

Before we go down to legal protection on social media, we should define social media. Current legal framework still does not have a clear image about what exactly social media is. Nowadays, social media not only represents "a form of computer-mediated communication" (Mclntyre, 2014, p.6) but also means "a mechanism for audience to connect, communicate, and interact" (Correa, Hinsley & Zuniga). According to the latest research, social media is defined as "web-based service that allow individuals, communications, and organizations to collaborate, connect, interact, and build community" (McCay-Peet & Quan-Haase, 2017). When lawmakers intend to enact a law about social media privacy, they can refer to the academic research related to the topic, and also clarity the applicability of the law, especially pointing out which social media site can be considered as the object of the law.

(3) Awareness

Social media now is users' online resume. What we post not only represent our personal life and experience, but also represent who we are. These contents may play an important role when we are seeking new job opportunities. For applicants, they should increase the awareness about online privacy. Instead of sharing all the content to the public, changing the privacy setting to only allow friends to see the post can reduce risks of disclosing personal information. In addition, when asked to provide social media account information in a job application, applicants should be aware that they have the right to turn down this request.

Reference

Taddicken, M. (2013). Privacy, surveillance, and self-disclosure in the social web: Exploring the user's perspective via focus groups. In F. Christian, B. Kees, A. Anders & S. Marisol (Eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 255-272). London: Taylor and Francis.

Abril, P. S., Levin, A. & Riego, A. D. (2012). Blurred boundaries: Social media privacy and the twenty-first-century employee. *American Business Law Journal*, 49(1), 63-124.

Visser, A., & Mulder, I. (2011). Emergent technologies for assessing social feelings and experiences. In N. H. Sharlene (Ed), *The Handbook of Emergent Technologies in Social Research*, (pp.369-393). New York: Oxford University Press.

Weber, R. H. (2013). How does privacy change in the age of the internet? In F. Christian, B. Kees, A. Anders & S. Marisol (Eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (pp. 273-293). London: Taylor and Francis.

McCay-Peet, L. & Quan-Haase, A. (2017) What is social media and what questions can social media research help us answer? In S. Luke, & Q. Anable (Eds.) The SAGE *Handbook of Social Media Research Methods* (pp.13-26). London: SAGE Publications.

Gilpin, D. R. (2011) Woking the twittersphere: Microblogging as professional identity construction. In P. Zizi, (Ed) *A Networked Self : Identity, Community And Culture on Social Network Sites*. (pp. 232-250) New York: Routledge.

Madden, M. (2012). *Privacy management on social media sites*. Retrieved from http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/

Dijck, J. (2013). *The culture of connectivity : A critical history of social media*. New York: Oxford University Press.

Moore, G. (1998). *Cramming More Components Onto Integrated Circuits*. Proceedings of the IEEE, 86(1), 82-85.

Hutchinson, A. (2017) *Top Social Network Demographics 2017*. Retrieved from http://www.socialmediatoday.com/social-networks/top-social-network-demographics-2017-infographic