Client Alert

December 2011

In This Issue:

Global Recruitment and Social Media Hiring Traps

This article first appeared in Law360 on December 16, 2011

Online reputation management has become big business. Recruiters and employers are at the heart of it all, mining social media information to determine who to head-hunt and whether to hire potential candidates. Global recruiters are particularly active in social media, given the ease of researching candidates in other jurisdictions.

There remains an interesting disconnect between what candidates think recruiters do, and what recruiters *actually* do during the hiring process: in 2009, while only 7% of US candidates, 9% of UK candidates, 13% of German candidates and 10% of French candidates believed that online data affected their job search, in fact, 70% of US recruiters, 41% of UK recruiters, 16% of German recruiters, and 14% of French recruiters have rejected candidates based on online data (Microsoft Study, "Online Reputation in a Connected World", January 2010, http://www.microsoft.com/security/resources/ research.aspx# reputation).

According to the Social Recruiting Survey published by Jobvite this past summer, 57.8% of US employers intend to recruit passive candidates to compete against other employers (http://recruiting.jobvite.com/resources/social-recruiting-survey.php). This means that even employees not currently looking for a position may be the subject of a social media search.

More recently, in September 2011, a US-based social media company interviewed 300 employers and published an infographic indicating that 91% of those employers surveyed use social networking sites to screen prospective applicants (http://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic/).

Add the fact that recruitment more often than not involves younger, Millenial employees, particularly the large recruitment programs for newly graduated entry-level candidates, and you've got plenty of online material to work through.

Global Trends

There are different cultural expectations and historical realities that impact tolerance levels for social media data "digging". This article will address legal limitations on background checks involving social media information by or about an applicant in select jurisdictions around the world. This will highlight the global trends that all employers, particularly multi-national employers, should consider when mining social media data in the recruitment and hiring process. These global trends include:

1) Data privacy laws in most jurisdictions limit not only the amount of online information an organization can mine about a potential candidate, but also the transfer of such data, particularly when it comes to data originating in the European Union; and

2) Discrimination and employment laws tend to restrict the gathering, and more often the use, of social media information.

Also, the terms of use of social media sites, such as Facebook, may restrict the access and use of online information for hiring purposes.

Many global organizations now outsource recruitment to another jurisdiction and/or centralize their global recruitment process into one jurisdiction. Employers must understand from where the source of liability concerning electronic information will flow. In some jurisdictions, such as Canada, privacy law has no limits on where an organization can transfer information, but the Canadian organization remains accountable for any privacy breaches in the foreign jurisdiction. In contrast, in the European Union, privacy laws prohibit data information from flowing across a border unless the originating European country is satisfied that the other jurisdiction offers adequate protection for personal information. This example highlights the importance of developing a global approach that understands the nuances of each jurisdiction.

The Americas

While Canada, the United States and the various jurisdictions in Central and Latin America all approach employment law differently, discrimination as well as evolving data privacy laws and related transfer of cross-border data remain the key concerns when gathering and using social media information during the recruitment process.

Canada

In Canada, discrimination claims are an employer's largest threat when mining social media for candidate information during recruitment. Human rights tribunals have confirmed that individuals are entitled to protection throughout the entire employment relationship, including during recruitment and probation. While it is acceptable for an employer to conduct an online background check on a potential candidate, it is contrary to the Canadian human rights law to make a hiring decision based on any of the legally protected grounds of discrimination.

There are a broad range of grounds of discrimination protected by Canadian human rights laws, including race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex (which includes pregnancy), sexual orientation, age, record of offences, marital status, family status and disability (which includes drug and alcohol addictions).

Canada has an equally robust privacy regime that will directly impact using information from social media sites during recruitment. In general, candidates have a right to privacy if the individual has made reasonable efforts to keep his or her social media information private. In other words, if the information is not already publicly available to any third party, penetrating any level of security could invite litigation.

The federal government regulates commercial privacy issues through the *Personal Information and Electronic Documents Act* (PIPEDA), except for British Columbia, Alberta and Quebec, which have each implemented their own privacy laws substantially similar to PIPEDA.

In all Canadian jurisdictions, privacy law requires that employers identify and document the purpose of collecting and using personal information. Generally, employers must obtain informed consent from an individual and can only use or disclose personal information thereafter for the purposes identified to the individual.

In October 2011, the British Columbia provincial government released the guideline, "*Social Media Background Checks*" (http://www.oipc.bc.ca/pdfs/private/Guidelines-SocialMediaBackgroundChecks.pdf). The guideline highlights certain risks associated with gathering information through social media background checks, including: the information may be gathered under a pretext of a social relationship; the information may be inaccurate, irrelevant or unreasonably broad for employment purposes; unauthorized third-party information may be inadvertently collected; and there are practical problems with a candidate's consent to gather information during the hiring process.

United States

While to date, the United States does not have a comprehensive data privacy law, it does have specific procedural requirements for conducting background checks under the Fair Credit Reporting Act (FCRA) and related state laws, such as the California's Investigative Consumer Reporting Agencies Act and the California Consumer Credit Reporting Agency Act.

The FCRA applies to "consumer reports" (which includes background checks) conducted by a "consumer reporting agency," but not to background checks conducted in-house. It requires, among others, that the candidate provide his or her written authorization before the potential employer conduct a background check. Furthermore, the potential employer must provide a pre-adverse action disclosure that includes a copy of the individual's background check report and a copy of "A Summary of Your Rights Under the Fair Credit Reporting Act" - a document prescribed by the Federal Trade Commission.

Furthermore, after an adverse action (here, the decision not to offer employment) has been taken, the individual must be given notice that the action has been taken, which must include contact information of the consumer reporting agency that supplied the report, a statement that the consumer reporting agency did not take the adverse action and cannot give specific reasons for it, and a notice of the individual's right to dispute the accuracy or completeness of the report and obtain an additional free consumer report upon request within 60 days.

Various companies in the US now offer comprehensive social media background checks. While privacy advocates raised concerns about such checks, the Federal Trade Commission recently held that one of these companies, Social Intelligence, can conduct social media background check if it conducts such checks in compliance with the FCRA requirements outlined above.

While the FCRA does not apply to social media background checks conducted in-house, such checks are often subject to restrictions under state or common law

privacy rules. For instance, it is often deemed a violation of privacy if an employer were to gain access to a candidate's social media information by posing as a friend.

In addition, US employers need to ensure not to violate Title VII (which prohibits discrimination based on race, color, national origin, religion or gender), the Age Discrimination in Employment Act (which prohibits discrimination against employees age 40 or over) or the Americans with Disability Act. State laws often add protected categories, such as in California, where sexual orientation, material status, pregnancy, cancer, political affiliation, genetic characteristics, and gender identity are all protected categories as well.

Furthermore, a 2008 federal law, the Genetic Information Nondiscrimination Act (GINA), limits an employer's ability to request genetic information, which includes conducting an internet search in a way that is likely to result in obtaining genetic information.

Latin America

At this point, there is little to no case law or statutory authority that impacts using social media in recruiting in Latin America, and data privacy laws are still evolving.

Argentinean law, for instance, does not have any restrictions on pre-hire background checks, and as such, there are no specific limitations on social media background checks either. Like in other jurisdictions, however, any pre-hire check should be conducted so as to avoid any discrimination based on race, religion, nationality, ideology, political affiliation, union membership, sex, economic standing, social condition or physical characteristics.

In countries such as Mexico, there are no specific laws that would apply to recruiting through social media. In fact, Mexican labour law only applies after the two parties commence the employment relationship as employer and employee. Furthermore, the Data Privacy Law that was issued last year does not contain restrictions for employers to use data contained in electronic media websites for recruiting processes. Rather, because the individual has uploaded his or her own information and made such data public, the Data Privacy Law does not consider such information in electronic media websites subject to protection. As a result, in Mexico there are no legal or judicial precedents that may impact whether an employer can use the information gathered from social media websites to determine whether to hire a specific candidate.

Europe

Background checks in the European Union (EU) are subject to numerous restrictions, mainly due to very stringent data privacy laws in the EU. The same is true when it comes to social media background checks, which many EU jurisdictions view as violating an employee's right to privacy. Even where permissible, numerous safeguards must be met not only to collect such information, but also to transfer it to jurisdictions that the EU views "unsafe" from a data privacy perspective, such as the United States.

France

In France, data obtained from public sources such as the media, news reports and similar publications may be collected and processed without need to obtain the candidate's consent. However, such checks may not be useful to a company because it is prohibited from making any employment-related decision based on data obtained during such searches, unless it has obtained specific authorization to do so from the French data protection authority (the CNIL). During the authorization procedure, the CNIL will evaluate (i) the company's justifications for processing the data, (ii) the legitimacy of its purpose, (iii) the proportionality of the data collected compared against the purpose of collecting it, and (iv) how the data collected may affect the candidate's interests/rights. This process can take between two to three months.

As to social media networks, due to the proportionality principle under French data privacy laws, only professional social networks can be searched (e.g., Viadeo, Plaxo, LinkedIn, etc.). Furthermore, candidates must be notified of the company's recruiting processes, including that the company or a third party will source information about the candidate through publicly available sources.

Employers are generally prohibited from requesting information based on potential discriminatory factors, which includes the applicant's gender, customs, sexual orientation, ethnic origin, nationality or race, political or religious beliefs, union involvement, external appearance, surname or state of health (unless the state of the applicant's health affects his/her ability to perform the job duties).

Finally, works council or employee delegate notification or consultation is generally required.

Germany

In Germany, like in France, background checks into social networks are only permissible with professional social networks, such as Xing or LinkedIn. Background checks are not permissible when it comes to other social networks, such as Facebook or MyLife. This rule is expressly set forth in the proposed news law on employee data privacy, although the proportionality principle set forth in the current data privacy law is read to imply similar restrictions.

Also, any works council has the right to be involved when the company sets up general principles on background checks (e.g., background check policies). Similarly, the data privacy officer should be informed.

Like in France, any discrimination must be avoided.

United Kingdom

Discrimination and privacy are also the key issues in the UK. Once an employer decides to conduct an online search about a candidate, the employer is "processing" data. Under Part 1 of the Employment Practices Data Protection Code, an employer is required to give a candidate the opportunity to comment on the accuracy of the data it is using in its employment decision. It is likely that conducting an extensive online search about a candidate without advising the candidate about the employer's online data gathering process would not comply with the Code.

The Information Commissioner's Office has not yet directly addressed the issue of using social media and online data in the recruitment process. Information gathered from online sources, however, may be captured by the Data Protection Act 1998 should the employer "process" the data by recording or using the information.

Asia Pacific

While social media is as prevalent in Asia Pacific as anywhere else in the world, discrimination and privacy laws have not yet had a significant impact on the use of social media information in the recruitment context.

Hong Kong

To date, there are no reported cases related to social media and recruitment in Hong Kong, although like in other jurisdictions around the world, Hong Kong is starting to see employees beiang terminated because of content that an employee shared on social media.

People's Republic of China

In China, while there is a general prohibition on employment discrimination based on ethnic background, race, gender or religion, there is no requirement to provide detailed reasons for not hiring a candidate. In practice, employers would likely not face any substantial risks if they declined to hire someone based on social media information.

An emerging area of potential risk is the prevalent use of microblogs such as Weibo.com by white collar employees in China. Workplace issues are a popular topic on the microblogs, and we anticipate that it is only a matter of time before specific employment law issues arise out of this widely used social media platform.

Philippines

Philippine law does not have any restrictions on pre-hire background checks, and as such, there are no specific limitations on social media background checks either. However, any pre-hire checks should be conducted so as to avoid any discrimination based on race, religion, nationality, union membership, sex, physical characteristics or medical condition, among others.

Conclusion

"Googling" an applicant is now an inevitable step in the application process for many employers. For global employers, developing a multi-jurisdictional protocol requires an awareness of the privacy, human rights and employment laws in each jurisdiction. It is crucial that global employers take steps to ensure compliance with applicable laws, including:

- develop a written policy that includes fair and non-discriminatory procedures on social media background checks;
- create a firewall so that somebody other than the decision-maker conducts the social media background check so as to avoid discrimination claims;

www.bakermckenzie.com

For further information please contact

Ute Krudewagen
+1 650 856 5577
Ute.Krudewagen@bakermckenzie.com

Lisa Stam
+1 416 865 6924
Lisa.Stam@bakermckenzie.com

- take steps to comply with local data privacy laws, including develop notices and consent forms for applicants, comply with any data privacy registrations, etc.;
- avoid using fake identities or engage in pretexting to gain access to information online;
- ensure any third party retained to conduct the searches thoroughly understands the nuances of the legal requirements in each relevant jurisdiction; and
- be prepared to disclose to a candidate the information used to determine whether to hire that individual.