Bloomberg BNA

Privacy and Security Law Report®

Big Data and Human Resources—Letting the Computer Decide?




By Susan McLean, Caroline Stakim, Hanno Timner and Christine Lyon

Employees are a company's greatest asset, but if the company gets hiring decisions wrong, employees could also be the company's greatest expense. Accordingly, recruiting the right people and retaining and promoting the best, while identifying and addressing under-achievers, is critical. Many organizations spend a lot of time and effort on human resources issues but do not have sufficiently detailed data to help them fully understand their employees and the challenges that can affect workforce planning, development and productivity.

Big data analytics can help to address these challenges, which explains why more and more HR departments are turning to them for a variety of purposes, for example, to: (i) identify potential recruits; (ii) measure costs per hire and return on investment; (iii) measure employee productivity; (iv) measure the impact of HR programs on performance; (v) identify (and predict) attrition rates and new hire failure rates; and (vi) identify potential leaders. Supporters also argue that big data analytics can help to provide evidence to de-bunk commonly held assumptions about employees that are wrong and based on biases.

Accordingly, the use of analytics promises many potential benefits for organizations, not only in terms of making improvements in talent identification and recruitment, but also in terms of workforce management. However, the use of data analytics in the HR sphere also raises some specific risks and challenges that companies need to consider, including increased exposure to discrimination claims, breaches of privacy law and reputational/brand damage. In this article, we will discuss some of the key factors companies need to bear in mind.

Susan McLean is of counsel in the London office of Morrison & Foerster LLP and specializes in technology and outsourcing law.

Caroline Stakim is an associate in the London office of Morrison & Foerster, where her practice focuses on employment and labor and employee privacy law.

Hanno Timner is a partner in the Berlin office of Morrison & Foerster and focuses on employment and data protection matters.

Christine Lyon is a partner in the Palo Alto office of Morrison & Foerster, where her practice focuses on privacy and employment law.

What Is Big Data?

Organizations have always accumulated information but, in this digital age, the amount of data being generated and retained is growing exponentially. IBM has calculated that 90 percent of the digital data that exists today was created in the last two years.[1] *In addition, historically, organizations may not have been able to draw value from the data that they held, particularly where such data were unstructured (and Gartner Inc. estimates that roughly 80 percent of all corporate data is unstructured*[2]*). However, new technologies now enable the analysis of large, complex and rapidly changing data sets comprised of structured, semi-structured or unstructured data. In short, ''big data'' is just data.*

[1] International Business Machines Corp., *IBM Big Data Success Stories*, ftp://ftp.software.ibm.com/software/data/sw-library/big-data/ibm-big-data-success.pdf (last visited Mar. 10, 2015).

[2] Gartner, Inc., *Major Myths About Big Data's Impact on Analytics* (Sept. 15, 2014), *available at* http://gtnr.it/1Ax9T87.

 ISSN 1538-3423

It's simply that we have more of it and we can do more with it.

I. Recruitment

Organizations are using big data analytics, for example, to identify candidates with the right skills and experience. New talent management systems can help organizations quickly search and analyze huge volumes of applicant data, *e.g.*, using concepts, not just key words. Organizations are also using analytics to analyze hiring data to help make changes in hiring strategy and recruitment collateral to attract more candidates and minimize attrition. There are two key stages that need to be considered in managing legal compliance with respect to these activities. First, there is the collection of data, and second, there is the analysis of the data and the formulation of resulting decisions.

A. Collecting and Processing Personal Data for Big Data Analytics

In terms of the collection of data, companies are increasingly mining candidate data from online sources, including job sites and social media sites, for the purpose of talent identification and recruitment. Privacy issues loom large because information collected about a proposed candidate will be considered personal data and may even contain sensitive personal information (*e.g.*, health data, ethnic origin and sexual orientation).

In Europe, where any recruitment activities involve the processing of potential recruits' personal data (and big data analysis of personal data will constitute processing), companies must give notice to potential recruits of the purposes for which data are intended to be processed and any other information that is necessary to ensure that processing is fair (*e.g.*, the names of data recipients).[3] Companies also must have a legal basis for processing the personal data (*e.g.*, consent). If a third party is engaged to carry out any processing, the potential employer will need to put in place with the third party a written contract with appropriate data protection provisions. There are some regional variations across Europe of which companies need to be aware. For example, in some countries (*e.g.*, Germany), even with an individual's consent, a potential employer is restricted in the background checks that it can carry out.[4] As a general rule, all background checks should be limited to the information strictly necessary to determine whether an applicant is suitable for a particular position, even if the applicant has consented. Additionally, through an online background check, information may only be collected if it is publicly available and the applicant does not have an apparent and justified interest in the exclusion of the information. Local employment laws may impose additional restraints. Accordingly, a company's processes may need to be modified from country to country.

Concerns over automated decision-making are sometimes raised and, certainly, automated decision processing is particularly problematic under European Union data protection law.[5] Accordingly, employers that use big data analytics in recruitment need to ensure that there is an element of human judgment involved in decision-making. It should not be (and typically is not) just a question of ''computer says yes'' but rather an informed decision based on the available data and the interpretation of the data.

In the U.S., if a company purchases background reports about candidates, the company will need to be mindful of the Fair Credit Reporting Act[6] and state consumer reporting laws.[7] These laws may come into play any time a company procures information about a candidate or employee from a third party that is in the business of supplying such information on a commercial basis, even if that information may be publicly available. Federal and state laws also limit the types of information that an employer may lawfully request or consider in making employment-related decisions, even if the information has been obtained lawfully.

Across Asia, rules regarding the use of personal data in terms of recruitment vary.

- In China, individuals are subject to a general right to privacy, and employers have certain obligations of confidentiality.[8] In general, employers are viewed as having a fairly broad ability to conduct background checks, although illegal or intrusive means may be viewed as a breach of privacy. However, third-party sources of information should be used with caution as few legitimate channels of information are available. The use of personal data from illegal channels can attract civil and sometimes criminal liability, and there have been a number of high-profile cases in recent months involving the illegal provision or acquisition of personal data.

- In Hong Kong, under the Personal Data (Privacy) Ordinance, personal information must be collected by lawful and fair means, and, if personal information will be used for a purpose other than that for which the data were originally posted (or a directly related purpose), consent will be required.[9] It may be acceptable to use without specific consent personal information that is published on a job-seeking or professional references social media site such as LinkedIn. However, personal information published on a personal social media site (such as a personal Facebook page) will generally require express consent.

- In Japan, personal information about applicants must be collected by appropriate and fair means.[10] As a rule, personal information about applicants must be collected directly from applicants or from third parties with the applicant's consent. Collec-

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, as implemented into local law.

[4] *See* sec. 32, para. 1, Federal Data Protection Act (Bundesdatenschutzgesetz) and corresponding court rulings, *e.g.*, Federal Labor Court decision of March 20, 2014, NZA 2014, 1131.

[5] Directive 95/46/EC, *supra* note 3, at art. 15.

[6] Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

[7] Examples include the California Consumer Credit Reporting Agencies Act (Cal. Civ. Code § 1785.1 et seq.) and the California Investigative Consumer Reporting Agencies Act (Cal. Civ. Code § 1786 et seq.)

[8] Tort Liability Law; Employment Services and Management Regulations.

[9] Personal Data (Privacy) Ordinance, (1996) Cap. 486, *available at* http://bit.ly/1BNmCaL.

[10] Japan's Law Concerning the Protection of Personal Information.

  PVLR ISSN 1538-3423

tion of sensitive personal information without express consent is generally prohibited. There is one exception: an employer may collect such sensitive information when such information is definitely necessary to achieve the employer's business, the employer has notified the applicant of the purposes of collection of such information and the employer collects such information directly from an applicant.

B. Avoiding Discriminatory Impact

Of course, as with all talent identification and recruitment activities, organizations also need to ensure that they do not act in a manner that could be considered discriminatory. In Europe, Directive 2000/78/EC establishes a general framework for equal treatment in employment and occupation, forbidding discrimination based on religion, belief, disability, age and sexual orientation.[11] Separate directives also forbid discrimination on the grounds of sex and race.[12] The principle of equal treatment means that there must be no direct or indirect discrimination on any of these grounds.

Likewise, in the U.S., laws such as Title VII of the Civil Rights Act of 1964,[13] the Age Discrimination in Employment Act,[14] the Americans with Disabilities Act[15] and a variety of other federal and state laws prohibit discrimination against applicants and employees based on protected characteristics such as race, age, sex, national origin, religion and disability. Employers may face liability under these laws if they unlawfully consider protected characteristics in their hiring or employment decisions. Employers may also face liability if they rely on screening or hiring practices that appear neutral on the surface but have a disparate impact on workers in protected classifications, such as disproportionately screening out older candidates or candidates with disabilities. This liability may arise even if the employer had no intent to discriminate or no knowledge of the discriminatory impact.

Organizations are generally aware of their obligations in this area in the context of traditional recruitment activities. However, they now need to appreciate their application in this new age of big data analytics. When organizations are identifying key words and concepts for a data collection exercise, they need to apply the same rigor that they would use when creating job advertisements, i.e., avoid any terms that could be considered directly or indirectly discriminatory (*e.g.*, ''recent graduate,'' ''highly experienced,'' ''energetic''). Organizations also need to be careful not to discriminate in terms of where they collect data from. Otherwise it could be a case of data that are ''discriminatory in, discriminatory out.''

In terms of an organization's analysis of the data collected, again it will need to ensure that its analysis and the decisions that it makes as a result of such analysis are not deemed discriminatory—in particular decisions that are based on predictive decision-making about candidates. Of course, it is very important that organizations do not blindly accept data without challenge. Given the size of the potential data pool, conclusions may well be based on correlations, rather than being determinative. Proper interpretation and assessment of the results of a big data exercise is essential. For example, organizations should be wary of any predictive decision-making that gives results that appear skewed in favor of certain types of candidates. For example, if a big data analytics exercise brings up a short list of potential candidates that have the same race, gender or other characteristic, that may suggest that there has been a discriminatory input at some point in the big data process. Although it may be difficult for a candidate to establish that a big data analytical exercise has been discriminatory, particularly given the potentially complicated algorithmic calculations involved and lack of transparency about those algorithms, organizations need to be mindful of the risks. In some cases, if a practice is determined to have a discriminatory impact, the burden may shift back to the employer to defend its methodology. Employers may also be required to disclose detailed information about their big data methodologies in the event of employment litigation or a government investigation. As a result, employers will want to be prepared to explain and, if necessary, justify their big data analytics methods.

C. Third-Party Rights

However, it is not just a question of compliance with privacy and HR issues because mining data from third-party sites, such as online job sites, could be a breach of their terms of use and, potentially, an infringement of intellectual property rights. Web scraping may also be considered a breach of applicable local cybersecurity laws that prohibit unauthorized access to computer systems (*e.g.*, the U.K. Computer Misuse Act 1990[16] and the U.S. Computer Fraud and Abuse Act[17]). Accordingly, organizations need to ensure that they have adequately addressed all potential legal risks prior to embarking on any data collection activities.

II. Workforce Management

The second area where analytics are being increasingly harnessed by HR departments involves the monitoring and analysis of data relating to employees. Again, this use of analytics throws up some particular issues that companies need to be aware of.

Many organizations already use analytics to obtain insights into their customers and target customers. Organizations are now seeking to obtain the same insights into their employees, which they can use to improve organizational efficiencies and drive productivity. This can help organizations to objectively evaluate their cur-

[11] Council Directive 2000/78/EC of 27 Nov. 2000 Establishing a General Framework for Equal Treatment in Employment and Occupation, 2000 OJ L303/16, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0078&from=EN.

[12] Council Directive 2006/54/EC of 5 July 2006 on the Implementation of the Principal of Equal Opportunities and Equal Treatment of Men and Women in Matters of Employment and Occupation (recast) (replacing the Equal Treatment Directive 76/207/EEC and the Equal Pay Directive 75/117/EEC); Council Directive 2000/43/EC of 29 June 2000 Implementing the Principle of Equal Treatment Between Persons Irrespective of Racial or Ethnic Origin.

[13] Civil Rights Act of 1964, 42 U.S.C. § 2000a (2012).

[14] Age Discrimination in Employment Act, 29 U.S.C. § 621 (2012).

[15] Americans with Disabilities Act, 42 U.S.C. § 12101 (2012).

[16] Computer Misuse Act 1990, *available at* http://www.legislation.gov.uk/ukpga/1990/18/contents.

[17] Computer Fraud and Abuse Act, 18 U.S.C. § 1001 (2012).

rent people management practices. Of course, if HR is going to become a more data-driven department, it will need to identify what data it holds on its employees and whether such data simply need to be joined up or more data need to be collected.

The collection of more data is very likely to involve increased monitoring of employees. The applicable rules relating to such monitoring vary across the world and, therefore, if a company is rolling out an HR analytics project, it will need to address monitoring and data collection on a country-by-country basis.

In Europe, employees have certain protections under the European Convention of Human Rights as incorporated into national law (*e.g.*, the right to respect for private life (Article 8), freedom of speech (Article 10) and freedom of association (Article 11)).[18] Employees also have protections under applicable data protection law. However, there are regional variations that employers need to address. For example, in certain countries, privacy regulators have issued specific guidance relating to the extent to which employers can monitor their staff (*e.g.*, see Part 3 of the U.K. Information Commissioner Office's ''Employment Practices Code''[19]). In countries such as Germany, work councils rules apply to the monitoring of staff.[20] Areas of particular concern include managing employees' legitimate expectations of monitoring, having appropriate notices/policies in place with employees and protecting employees' rights against discrimination for certain off-duty activities, *e.g.*, religious activities and trade union and political activities.

In the U.S., restrictions on monitoring arise under federal laws including the Electronic Communications Privacy Act, Stored Communication Act and Computer Fraud and Abuse Act,[21] and state laws that restrict certain types of monitoring activities, such as seeking to gain access to personal social media of applicants or employees.[22]

In Asia, there are similar restrictions on monitoring.

- In China, while employers are not restricted from monitoring publicly available information about employees, monitoring employees' computer use in the workplace may be more susceptible to legal challenge.[23] However, an employees' right to privacy would be balanced against an employer's statutory duties.

- In Hong Kong, applicable law requires that monitoring must serve a legitimate purpose that relates to the function and activities of the employer.[24] Monitoring measures must be necessary to meet that purpose and must be confined to an employee's work. Personal data collected must be kept to the minimum necessary to protect the interests of the employer or to effectively address those risks inherent in the lawful activities of the employer. Monitoring must be carried out by the least intrusive means and with the least harm to the privacy interests of the employees. Employers are also required to document monitoring in a formal privacy policy setting out the employer's purpose, and employers must notify employees of the policy before commencing monitoring.

- In Japan, applicable law requires that if monitoring is implemented, an employer should: (i) establish in advance the in-house rules that stipulate the implementation of monitoring; (ii) specify in advance the purpose of the monitoring and notify workers of such purpose plus the relevant in-house regulations; (iii) establish the responsible official for the implementation of monitoring and its authority; and (iv) check that monitoring is properly implemented.[25]

When carrying out big data analysis, employers will need to ensure that they avoid automated decision-making and otherwise process such employee data fairly and in accordance with applicable privacy and employment laws. Again, inputs and algorithms need to be carefully set up to ensure that they do not discriminate, and organizations need to avoid any decision-making (predictive or otherwise) that could be considered discriminatory.

Of course, big data analytics are not a panacea. Organizations are complex, and human judgment is always going to be needed to interpret the data in context, taking into account relevant factors such as local market conditions. Complex algorithms may help to identify an organization's highest performing employees who may be likely to leave the organization in the next 12 months, but HR departments will still need to tread carefully in deciding how to respond (or not) to such data.

Also, it is clear that better, more informed data about your workforce can help drive change in the business, but only if the business is actually prepared to embrace that change. Organizations have to be open to accept what the data are telling them, be prepared to change their systems and processes to take account of the data science and acknowledge that a period of adoption is likely to be needed. In addition, companies cannot underestimate the expense and effort of any training programs that may be required to roll out an operational

[18] Consolidated version of Convention for the Protection of Human Rights and Fundamental Freedoms, *available at* http://conventions.coe.int/treaty/en/treaties/html/005.htm.

[19] ICO, *The Employment Practices Code* (Nov. 2011), *available at* https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf.

[20] *See* Sec. 87 para. 1 No. 6 Works Council Constitution Act (Betriebsverfassungsgesetz).

[21] Electronic Communications Privacy Act, 18 U.S.C. § 2510 (2012); Stored Communications Act, 18 U.S.C. § 2701(2012); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

[22] *E.g.*, Cal. Labor Code § 980.

[23] In China, a number of laws can apply to the monitoring of employees' e-mail and computer usage. For example, Article 3 of China's Administration of E-Mail Services Procedures protects the privacy of a citizen's e-mail, but it also provides that a person is permitted to send e-mail only if authorized by the owner of the computer system.

[24] Hong Kong's Personal Data (Privacy) Ordinance, as supplemented by the Privacy Guidelines: Monitoring and Personal Data Privacy at Work issued by the Office of the Privacy Commissioner of Personal Data, Hong Kong, *available at* http://media.mofo.com/docs/mofoprivacy/Japan/METI%20-%202007%20Revised%20Guidelines_v2.pdf.

[25] Japan's Law Concerning the Protection of Personal Information, as supplemented by the Ministry of Economy, Trade and Industry (METI) Guidelines Targeting Economic and Industrial Sectors With Regard to the Law Concerning the Protection of Personal Information, *available at* http://media.mofo.com/docs/mofoprivacy/Japan/METI%20-%202007%20Revised%20Guidelines_v2.pdf.

  PVLR ISSN 1538-3423

change that may be inconsistent with traditional thinking.

Of course, it is not only a question of legal compliance. In this age of international business, the war for talent in certain sectors has never been greater, and companies want to attract and retain the best people. Accordingly, companies need to strike a balance between monitoring staff for the purpose of people management analytics and the organization being seen as a ''creepy'' employer, where employee movements and communications are extensively monitored Big Brother style. From the employee's perspective, much may depend on the nature and extent of data being collected and what the employer plans to do with the data. In order to foster employee engagement and trust in analytics, organizations also need to explain to their workforce how those analytics will directly benefit the employees, for example, in terms of better engagement, transparency and empowerment.

Conclusion

Big data analytics may offer HR departments the ability to make better, more objective, data-driven decisions about recruitment and employees. However, the value of a big data project will depend very much on the quality of the inputs and project parameters and the careful interpretation of the results. HR departments will need to have appropriate analysis in-house or hire appropriate service providers to help them design the appropriate big data program and interpret the resulting data. Of course, if a company uses a third-party provider for the provision of HR big data technology and analytics services, there will be other legal issues it will need to consider, in particular in respect to commercial arrangements (*e.g.*, many HR analytics providers offer analytics on the basis of cloud-based Software as a Service) and intellectual property rights and data ownership.