HR Data Privacy in the Era of Big Data

By Dr. Donald F. Harris, HR Privacy Solutions

We live in an unprecedented era when personal data is being hoovered-up, stored and made accessible for profile generation and analysis in a little-disclosed manner, by government security agencies, corporations, criminals, political parties, fundraisers, researchers, and a host of other parties. While the potential benefits are profound, so are the dangers, and each is only compounded by the dawning age of ubiquitous computing and the Internet of Things. Our societies have scarcely begun to sort things out, with legislation to protect privacy and individuals lagging painfully behind technological and economic advancements.

Against this larger, unsettled, and often disturbing background, the privacy issues confronting employers, while not insignificant, seem far more manageable. Let's first consider those impacting multinational companies and then turn to those any company anywhere needs to attend to.

For companies with an international workforce, complying with transborder data flow (TBDF) requirements remains a top concern, with Europe's lead in this regard being followed by countries as diverse as Mexico, Australia, and Russia. One of the main means of meeting European TBDF requirements, the Safe Harbor[1] program, has long been under assault by critics. In 2013, following outrage over Snowden's revelations of NSA mass surveillance, the European Commission called for 13 specific reforms to strengthen Safe Harbor and has been negotiating ever since with the U.S. to secure them. Notwithstanding recent statements of optimism from both sides[2] – we heard similar statements last summer – the future of Safe Harbor is uncertain.

Should the program be suspended, as the EU Parliament has called for and the Commission has threatened, the 4,000 or so U.S. companies participating in the program would have no legal means of importing personal data from Europe, including that of employees. The impact upon these companies would be severe, since the associated data transfers would have to stop until an alternative compliance mechanism, such as the execution of model contracts or the establishment of Binding Corporate Rules, was achieved. Many HR programs and strategies would be totally disrupted in the meantime. Prudent Safe Harbor participants are preparing for this possibility.

The expected enactment of the new EU General Data Protection Regulation (GDPR) by the end of 2016,[3] replacing the 1995 Data Protection Directive, will require most U.S. companies with European employees to significantly upgrade their privacy programs. For example, companies will have to be able to demonstrate, through documented policies, procedures, and oversight programs both in Europe and at home, that they comply with the GDPR. Failures to comply will be punishable not by a slap on the wrist, as at present, but with substantial fines that could range from two percent to five percent of a company's total annual revenues. Once again, prudent companies are beginning to laying the groundwork for GDPR compliance.

Another development impacting companies with international employees is the significant ratcheting-up of enforcement actions. Recent years have seen a steady advance in the cooperation, collaboration, and powers of data protection authorities around the world. By pooling their resources, lesser authorities have been able to take on big tasks. For example, the small Belgian privacy authority has taken the lead in Europe in going after Facebook and just recently filed a law suit against the company over its tracking of non-users.[4] The DPAs are increasingly employing the *name-and-shame* tactics and bigger fines typically associated with regulatory enforcement in the U.S. They are also becoming more effective, bringing an end to years of stonewalling by U.S. tech giants and compelling them to change their practices. With foreign courts also becoming increasingly involved, as in the *Google Spain v. AEPD and Mario Costeja Gonzalez* right-to-be-forgotten case,[5] ignoring or attempting to fly under the radar of enforcement is an increasingly risky proposition.

For all companies, whether multinational or not, other key privacy issues include the prevention and remediation of data breaches; avoiding use of irrelevant or questionable data in employment decisions; promotion of wearable devices; tracking and surveillance of employees; and the risks of going overboard with *big data analytics*.

Breaches of employee data remain an enormous headache and liability for employers, as U.S. states continue to enact ever stricter, one-off obligations around prevention and response, as other countries (e.g., Canada, the Netherlands, and in the near future, all of Europe) follow the U.S. lead by adopting breach notification laws, and as lawsuits by employees multiply. The staggering compromise of employment and sensitive background investigation data reported by the U.S. Office of Personnel Management in June, jeopardizing the privacy of up to 22 million individuals and the security of the nation, should be a wake-up call to all employers.[6] Expanded security training for employees, more technical resources such as data loss prevention software, and a radical rethinking of security for the most sensitive personal data should be pursued.

The use of irrelevant, questionable, and sometimes inaccurate personal data to make employment decisions has emerged as a significant social issue. In the U.S., over 100 cities and 18 states have passed "ban the box" laws that prohibit employers from inquiring about the criminal histories of job applicants on employment applications.[7] At least 21 states have enacted laws banning employers from accessing the social media accounts of applicants and employees.[8] In Canada, privacy regulators in British Columbia and Ontario have forced the police to stop providing irrelevant information in their files to employers. In the UK and Ireland, regulators have cracked down on the attempt by employers to skirt privacy laws and determine the criminal history of applicants via what is called "enforced data subject access." Employers need to bear in mind that the accuracy and relevancy of personal data are fundamental privacy principles.

Many employers are attempting to incorporate the growing interest in fitness wearables, such as Fitbit, into their wellness initiatives, in order to improve the health of employees and restrain healthcare costs. Some observers believe that employers may soon be mandating the use of such devices,[9] but HIPAA in the U.S. and privacy laws abroad make this unlikely. However, with appropriate planning and privacy safeguards in place, such as ensuring that employers, insurers, and unidentified third parties do not have access to individually-identifiable data from the devices, both employers and employees should be able to reap the potential benefits of wearables.

Tracking and surveillance of employees, a perennial privacy issue, has traditionally focused on the monitoring of employee communications, computer, and Internet usage. In the absence of laws to the contrary, and in spite of considerable arbitration and litigation in this area, employers in the U.S. generally have a free hand in carrying out such surveillance. Not so in any of the more than 100 countries with comprehensive data protection laws; in these nations such monitoring may only be carried out, if permitted at all, with adequate notice to employees and sometimes to works councils and data protection authorities as well. Tracking of location data generated by company-issued mobile devices – data which can be quite sensitive and may reveal activity beyond working hours – is only a more recent extension of these traditional forms of employee surveillance.

Surveillance is being taken to a whole new level by what is known as the Quantified Workplace movement. Firms such as Evolv, Sociometric Solutions, and Steelcase supply technologies and products to track the behavior, movements, and interactions of employees, running analytics on data collected by traditional means, new data gathered from sensor-equipped ID badges, furniture and buildings, and performance measures. The payoff in productivity improvements from such Frederick Taylor-like approaches can be significant.[11] However, these technologies need to be deployed carefully, ensuring that employees understand what data is being collected, who will have access to it, and how it will be used. Unless privacy concerns are met, the workplace could be transformed by overreaching quantification analytics into the equivalent of Jeremy Bentham's debilitating and dehumanizing *panopticon* prison.

Technology is evolving at an unprecedented pace, with both the workplace and HR often in the vanguard of adaptation. Getting one's privacy house in order is a critical prerequisite to being nimble and effective in introducing new technologies.

Endnotes

[1] Hogan Lovells blog, "European Commission Calls for Data Transfer Reforms," November 27, 2013, (http://www.hldataprotection.com/2013/11/articles/consumer-privacy/european-commission-calls-for-data-transfer-reforms/).

[2] Loek Essers, *TechWorld*, "EU, US officials close in on broad privacy accords," June 4, 2015, (http://www.techworld.com.au/article/576586/eu-us-officials-close-broad-privacy-accords/).

[3] Olivier Proust, Fieldfisher blog, "EU Council of Ministers Adopts General Data Protection Regulation," June 17, 2015, (http://privacylawblog.fieldfisher.com/2015/eu-council-of-ministers-adopts-general-data-protection-regulation).

[4] Samuel Gibbs, *The Guardian*, "Belgium takes Facebook to court over privacy breaches and user tracking," June 15, 2015, (http://www.theguardian.com/technology/2015/jun/15/belgium-facebook-court-privacy-breaches-ads).

[5] *SC Magazine*, "A year of trouble and strife for Google and the 'Right to be Forgotten'," May 14, 2015.

[6] Jeff Goldman, *eSecurity Planet*, "OPM Breach Hits 22 Million People, Director Resigns," July 13, 2015, (http://www.esecurityplanet.com/network-security/opm-breach-hits-22-million-people-director-resigns.html).

[7] Michelle Natividad Rodriquez and Nayantara Mehta, National Employment Law Project, "Ban the Box: U.S. Cities, Counties, and States Adopt Fair Hiring Practices," July 1, 2015. (http://www.nelp.org/publication/ban-the-box-fair-chance-hiring-state-and-local-guide/).

[8] National Conference of State Legislatures, "State Laws About Social Media," June 12, 2015, (http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx).

[9] Parmy Olson, "More Bosses Expected to Track Their Staff Through Wearables in the Next 5 Years," Forbes, June 1, 2015, (http://www.forbes.com/sites/parmyolson/2015/06/01/wearables-employee-tracking/).

[10] Hannah Kuchler, *Financial Times*, "Data pioneers watching us work," February 17, 2014, (http://www.ft.com/intl/cms/s/2/d56004b0-9581-11e3-9fd6-00144feab7de.html#axzz3fyd5ManZ).

[11] Josh Bersin, *Forbes*, "Quantified Self: Meet the Quantified Employee," June 25, 2014, (http://www.forbes.com/sites/joshbersin/2014/06/25/quantified-self-meet-the-quantified-employee/).

About the Author

Dr. Donald F. Harris is president, HR Privacy Solutions, a management consulting practice that has helped over 30 leading multinational clients meet the challenges posed by global privacy laws. Founder of IHRIM's Privacy Committee in 1996 and a Summit Award winner, he is an internationally known expert, author and speaker on HR data privacy issues. He can be reached at ***donaldharris@hrprivacy.com***.