A Timely Analysis of Legal Developments

ASAP®

January 7, 2014

Workplace Privacy 2014: What's New and What Employers May Expect

By Philip Gordon

New laws that went into effect on January 1, 2014, are a harbinger of what employers may expect to see in the coming year regarding workplace privacy: more restrictions on access to applicants' and employees' criminal history, credit information, and personal social media content. To further complicate the challenges of addressing privacy in the workplace, employers will be required to grapple with next-generation issues raised by the use of social media as a business tool and the increasing adoption of "bring-your-own-device" (BYOD) programs. As reflected in the summary below, the ever-shifting balance between employer prerogative and employee privacy likely will continue to move in a direction that favors employee privacy.

Criminal History Information: With the start of 2014, Minnesota and Rhode Island joined the wave of jurisdictions that have "ban-the-box" legislation. These laws generally prohibit employers from requesting criminal history information in the employment application. Ban-the-box laws have also been enacted in Buffalo (NY), Hawaii, Massachusetts, Newark (NJ), Philadelphia (PA), and Seattle (WA). Similar bills are pending in 26 states. These laws create challenges for employers because they establish both varying rules on the point in the hiring process at which an employer can request criminal history information and different procedural requirements surrounding such requests. Also effective on January 1, 2014, is a new California law that prohibits employers from asking about or considering information concerning applicants' criminal convictions that were judicially dismissed or ordered sealed. This new law adds to a growing list of state law restrictions on employers' inquiries into criminal history information—*in addition* to restrictions on inquiries about criminal history in the employment application. In addition to new legislation in this area, employers likely will also see continued aggressive enforcement by the Equal Employment Opportunity Commission (EEOC) regarding employers' use of criminal history for employment decisions and increased litigation by the plaintiffs' class action bar which won several seven-figure settlements in 2013 based on employers' alleged violations of the federal Fair Credit Reporting Act (FCRA) when conducting criminal history checks.

Credit Information: On January 1, 2014, regulations implementing Colorado's Employment Opportunity Act became effective. The law and its implementing regulations are similar to laws enacted in nine other states that restrict the use of credit information for employment purposes. These laws generally prohibit employers from procuring credit information on applicants and employees unless the information is "substantially job related." However, the laws establish

materially different definitions of that key statutory term. The states that have enacted such laws, in addition to Colorado, include California, Connecticut, Hawaii, Illinois, Maryland, Nevada, Oregon, Vermont, and Washington. Similar bills are pending in 35 states. In addition, in December 2013, U.S. Senator Elizabeth Warren introduced a bill that would impose restrictions on employers' use of credit information for employment purposes that are more stringent than any of these state laws.

Social Media Passwords: On January 1, 2014, Oregon became the twelfth state with a "social media password protection" law, joining Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Utah, and Washington. These laws share one common thread: they all prohibit employers from asking applicants for their user name, password or other log-in credentials for their personal social media accounts, and all of the laws, except New Mexico's, impose the same prohibition with respect to employees. Unfortunately, beyond that, the laws vary materially in terms of prohibited conduct, exceptions, and remedies. Employers will likely face increasing complexity in this area in 2014 as bills addressing access to applicants' and employees' personal social media are pending in 15 states.

Other Social Media Issues: Since January 2011, the National Labor Relations Board (NLRB or Board) has repeatedly struck down provisions of employers' social media policies and reversed employer discipline of employees based on employees' personal social media activity. According to the Board, these employers violated Section 7 of the National Labor Relations Act (NLRA) by implementing policies that interfered with employees' right to discuss the terms and conditions of employment or by disciplining employees for exercising that right in social media. Because social media have become an integral part of daily life for so many employees, in 2014, employers will continue to confront these issues. Employers also may encounter a new set of issues arising from their growing reliance on social media to advance their business interests. Recent decisions by the NLRB's administrative law judges and recent statements by the NLRB's recently confirmed General Counsel suggest that if employers allow employees to use corporate social media platforms, such as Yammer or Chatter, or corporate social media pages for non-business purposes, the NLRB will attempt to impose the same restrictions on employers that it has applied to employees' personal social media activity. In other words, without carefully drafted policies or terms of use, employers run the risk that corporate-sponsored social media sites could be subverted for employees' complaints about the terms and conditions of employment.

Bring Your Own Device: The "consumerization of IT" will continue to expand in 2014 as more employers hope to reap savings from employees using their personal devices, rather than corporate-owned devices, to conduct their employer's business. These "bring your own device" programs pose fundamental challenges for employers seeking to balance the need to safeguard customer and corporate data without unlawfully accessing employees' personal information. While many employers have addressed the balance through BYOD policies and user agreements, maintaining that balance will become only more challenging to maintain in 2014 from an operational perspective as employees increasingly rely on mobile apps to store sensitive information about themselves, such as blood pressure, blood sugar level, and heart rate. For multinational employers, the roll-out of BYOD programs in 2014 to their employees in the European Union and other jurisdictions with broad data protection laws can create even more substantial challenges. In many of these jurisdictions, employers face greater restrictions than in the U.S. on access to an employee's personal device. In addition, employers must implement systems that will permit data subjects to obtain access to, and update, the data subject's personal data even when it is stored on an employee's personal device.

In sum, it is likely that two major trends will continue to play out in 2014 in the area of workplace privacy, and in a direction that favors employees. First, legislators, enforcement agencies, and the plaintiffs' bar will likely continue their efforts to narrow the scope of information that employers can consider when making employment decisions about applicants and employees. Second, technology will continue to blur the lines between work and personal life, with personal life expanding into work life—not the other way around. However, the widening scope of the NLRA and the increasing number of countries with broad data protection laws will compel employers to tolerate this "intrusion" of personal life into work.

Employers should consider the following steps in response to these trends:

- Review existing practices for collecting and using criminal history, credit and personal media information about applicants and employees and implement policies to ensure compliance with state law restrictions on the collection of such information as well as with the federal Fair Credit Reporting Act's background check requirements;
- Implement a social media policy, or update the organization's existing policy, to address recent NLRB decisions with respect to *both* employees' personal social media activity and employees' social media activity on the employer's behalf;

- Require that all U.S. employees execute a BYOD user agreement before permitting them to use a personal mobile device to conduct company business;
- Before rolling out a BYOD program to non-U.S. employees, evaluate whether local law will permit the employer to take the necessary steps (such as, access to, and monitoring of, the personal device and remote wipe) to safeguard corporate and customer data and develop systems for complying with requests by data subjects to exercise their rights with respect to data stored on employees' personal devices.

This article originally ran in the IAPP's Privacy Tracker blog.

Phillip Gordon, Chair of Littler Mendelson's Privacy and Data Protection Practice Group, is a Shareholder in the firm's Denver office. If you would like further information, please contact your Littler attorney at 1.888.Littler or info@littler.com, or Mr. Gordon at pgordon@littler.com.