Insight

IN-DEPTH DISCUSSION

May 27, 2015

Connecticut Restricts Employer Access to Personal Social Media, E-mail and Online Retail Accounts of Employees and Applicants

By George O'Brien and Philip L. Gordon

On May 19, 2015, Connecticut Governor Dannel P. Malloy signed into law a new statute restricting an employer's ability to gain access to social media, e-mail and other personal online accounts of employees and job applicants. Connecticut is the twentieth state to enact such legislation. Connecticut's law generally is in line with similar state laws, having no outlier provisions that could pose a particular compliance challenge for multistate employers.

Public Act 15-6 (the Act) will take effect on October 1, 2015. It applies to private and public employers of any size, including the state and political subdivisions of the state, such as municipalities. The law does not apply, however, to a state or municipal law enforcement agency when it conducts a pre-employment investigation of law enforcement personnel.

The Act prohibits an employer from requesting or requiring an employee or applicant to provide the employer with a user name and password, password standing alone, or other means of authentication for accessing a "personal online account." This means an online account used by the employee or applicant exclusively for personal purposes unrelated to any business purpose of the individual's employer or prospective employer. The term applies to electronic mail, social media and "retail-based" (or online shopping) websites. It does not include any account "created, maintained, used or accessed" by the employee or applicant for a business purpose of an employer or prospective employer.

The Act also prohibits an employer from requesting or requiring that an employee or applicant authenticate or access a personal online account in the presence of the employer (*i.e.*, "shoulder surf"), and from requiring that an employee or applicant invite the employer, or accept an invitation from the employer, to "join a group affiliated with" the personal online account of the employee or applicant. Unlike similar laws in some states, Connecticut's law does not expressly prohibit an employer from requiring an applicant or employee to change his or her privacy settings for a personal online account in a way that would permit the employer to view the individual's online content. However, such an approach arguably would be inconsistent with the spirit of the new law.

Employers are prohibited from discharging, disciplining, discriminating against, retaliating against or otherwise penalizing an employee who refuses an employer's request made in violation of the foregoing restrictions, or who initiates a verbal or written complaint to a "public or private body or court" concerning such a violation. The language of this prohibition is so broad that it appears it could include disciplinary actions taken by an employer who was unaware of the employee's refusal or complaint. A more narrowly drafted provision prohibits employers from failing or refusing to hire an applicant "as a result of" the applicant's refusal to provide online account access improperly requested by the employer.

The Act contains several significant exceptions to the general prohibition. Most importantly for employers, the Act, like many similar laws in other states, contains a relatively broad exception for workplace investigations. That exception applies to investigations conducted by employers to ensure compliance with state or federal laws, regulatory requirements, or prohibitions against work-related employee misconduct. Such an investigation must be based on the employer's "receipt of specific information about activity on an employee or applicant's personal online account." Employers can also conduct investigations based on receipt of specific information about an individual's unauthorized transfer of the employer's proprietary information, confidential information or financial data to or from the individual's personal online account. While the employer may conduct the investigation by shoulder surfing the employee's account, the employer may not require the employee or applicant to disclose the user name and password, password standing alone, or other means of authentication for accessing the account.

Another exception ensures continued access by employers to employer-provided online accounts and electronic devices. That exception permits an employer to request access to any account or service provided by the employer "or by virtue of the employee's work relationship with the employer" or that the employee uses for business purposes. It also permits the employer to require access to any electronic communications device that the employer supplied or paid for in whole or in part. As defined in the Act, this includes any electronic device capable of transmitting, accepting or processing data, including a computer, computer network and computer system, and a cellular or wireless telephone. In other words, the Act imposes no restriction on employers' access to information stored in employer-provided accounts or devices.

The Act also imposes no restriction on employers' monitoring online communications using the employer's electronic resources, for example, to ensure compliance with FINRA regulations on social media use by registered representatives. More specifically, the Act expressly allows employers, consistent with state and federal law, to monitor, access or block electronic data stored on an electronic communications device paid for in whole or part by the employer or traveling through or stored on the employer's network. There is also a general authorization for employers to comply with the requirements of state or federal statutes, rules or regulations, case law or "rules of self-regulatory organizations," such as FINRA.

The Connecticut Labor Commissioner is empowered to enforce the statute when an employee or applicant files a complaint alleging a violation. The commissioner is to investigate such complaints and may hold hearings concerning them. Upon finding that an employee is aggrieved by a violation, the commissioner may levy a civil penalty up to $500 for a first violation and $1,000 for each subsequent violation, and award the employee "all appropriate relief including rehiring or reinstatement to his or her previous job, payment of back wages, reestablishment of employee benefits or any other remedies that the commissioner may deem appropriate."

In the case of an aggrieved applicant, the commissioner may levy a civil penalty of up to $25 for a first violation and $500 for each subsequent violation. The statute does not authorize the commissioner to order an employer to hire such an applicant. Any employee or applicant who prevails in such a hearing "shall be awarded reasonable attorney's fees and costs."

The statute provides for appeals to the Superior Court from such decisions by the commissioner and also authorizes the commissioner to request the Attorney General to bring civil actions to recover the civil penalties that the commissioner has levied for violations. Like similar laws in most jurisdictions, the Act does not provide for a private right of action.

Recommendations for Employers

Connecticut employers should consider training employees whose job responsibilities intersect with the Act on the Act's key requirements. Training should emphasize that the law prohibits requesting access, in any manner, to an applicant's personal online accounts. Connecticut employers should note, however, that the Act does not prohibit employees involved in the job application process from accessing an applicant's publicly available on-line content or from using that content to make employment decisions, albeit such restrictions may be needed to comply with anti-discrimination and other laws. In addition, employees responsible for conducting investigations should be trained on the circumstances when a request for access to personal online content is permissible and the Act's limitations on such requests.