InsideCounsel.com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
June 6, 2014


Don't Ask, Don't Entail: Watch out for new workplace data privacy laws

Federal law can complicate things, as may be seen in the case of Ehling v. Monmouth-Ocean Hospital Service Corp.

BY RICHARD MARTINEZ , MAHESHA SUBBARAMAN

In our last article, we discussed the importance of developing privacy and cybersecurity policies to address potential risks arising from employees who use third-party file-hosting services to store company data. We thereby emphasized the reality that if you have employees with laptop computers, some proportion of them is bound to be storing company data on assets that your company does not control. In this article, we consider an inevitable corollary to that reality: Some proportion of your employees (probably a significant portion of them) are using online social media — from Facebook to Twitter to Instagram, to name a few — in ways that your company does not control.

Now, in developing privacy and cybersecurity policies to address this reality, it is important to recognize that such policies must serve not only to protect company confidences, but also to ensure that company personnel do not inadvertently violate a host of new state laws protecting employee use of social media. For example, on May 23, 2014, Louisiana Governor Bobby Jindal signed into law the Personal Online Account Privacy Protection Act. Under the Act, an employer may not "[r]equest or require an employee or applicant for employment to disclose any username, password, or other authentication information that allows access to the employee's or applicant›s personal online account." "Personal online account" includes any online service that an employee "uses exclusively for personal communications unrelated to any business purpose of the employer." In short, under Louisiana law, it is now generally illegal for employers to ask or require that employees hand over the passwords to their private Facebook or Twitter accounts.

Louisiana joins a growing list of states to enact this kind of legislation. The National Conference of State Legislatures reports that so far in 2014, workplace data privacy laws have been introduced or are pending in 28 states. As for the dozen-plus states that have already enacted workplace data privacy laws — including California, Delaware, Illinois, and Wisconsin — employers face significant liability if they fail to comply with these laws. For example, under Maine's "Social Media in the Workplace" law, if an employer requires an employee to disclose their login information "to a social media account or personal e-mail account," that employer may be subject to a private civil action in which the affected employee may recover three times any wages the employee has lost, civil damages of up to $1,000, and attorney's fees. Maine's law further empowers the state's attorney general to enforce such sanctions.

But such laws are not without exceptions. For example, under Louisiana's new law, employers do not face liability for "[c] onducting an investigation or requiring an employee or applicant to cooperate in an investigation . . . [i]f the employer has specific information about an unauthorized transfer of the employer›s proprietary information, confidential information, or financial data to an employee's or applicant›s personal online account." And under Utah's Internet Employment Privacy Act, an employer is not prohibited from "disciplining or discharging an employee for transferring the employer›s proprietary or confidential information or financial data to an employee›s personal Internet account without the employer›s authorization." The existence (or lack) of such exceptions in state workplace data privacy laws thus raises important complications for companies to consider in crafting a comprehensive policy governing employee use of social media—particularly if the company's employees are located in a variety of states with differing standards of workplace data privacy protection.

Federal law also complicates things, as may be seen in the case of *Ehling v. Monmouth-Ocean Hospital Service Corp.* In Ehling, a registered nurse sued her employer — a non-profit hospital service corporation — after being disciplined by her employer for an inflammatory wall post on her Facebook account. In this regard, the nurse alleged (among other things) that her employer's accessing of the Facebook wall post violated the federal Stored Communications Act (SCA). The SCA imposes civil liability on those who obtain unauthorized access to "a facility through which an electronic communication service is provided."

Ultimately, the U.S. District Court for the District of New Jersey granted summary judgment to the employer on the SCA claim. The district court reasoned that while the employee's "non-public Facebook wall posts [were] covered by the SCA," the employer was not liable under the SCA because of undisputed evidence showing that the employer obtained the wall post at issue via a voluntary disclosure by one of the employee's colleagues. The employer thus obtained the Facebook post without "coercion or pressure" — and the plaintiff failed to produce any evidence showing that her colleague "provided [the] information [to the employer] in exchange for compensation (or some other benefit)." However, Ehling indicates that employers who do use coercion or pressure to access to an employee's social media account or non-public postings may face significant liability under federal law (i.e., the SCA) as well as state law.

Employees lead professional and private lives, and respecting both is the key to crafting an effective privacy and cybersecurity policy that addresses the risks posed by employee use of social media. Of course, striking this balance is no easy task, given the constantly evolving nature of social media and the considerable lack of controlling judicial precedent. Nevertheless, as cases like *Ehling* and a growing tide of state legislation make clear, in-house counsel cannot afford to wait in dealing with this trend. Nor can counsel afford to ignore the unmistakable message of this trend: that when it comes to an employee's social media accounts, a company access policy of "Don't Ask, Don't Entail" may be the best place to start.

About the Authors

Richard Martinez
Richard Martinez is a trial attorney at Robins, Kaplan, Miller & Ciresi L.L.P. Rick's practice focuses substantially on technology, primarily in the areas of intellectual property litigation. His practice is also active in matters before the International Trade Commission, and in the areas of cyber security, data privacy, and information law.

Mahesha Subbaraman
Mahesha Subbaraman is an associate at Robins, Kaplan, Miller & Ciresi L.L.P., focusing on data privacy, cybersecurity issues and complex business litigation. mpsubbaraman@rkmc.com.

Reprinted with permission from InsideCounsel