Facebook Password Bills Are Pointless And Unfair

Related Professionals

Jackie Ford

Related Services

Employment Litigation

Labor and Employment

AUTHORED ARTICLE | 7.11.2013

Law360

Jackie Ford, partner in the Vorys Houston and Columbus offices, authored an article for *Employment Law360* about laws being passed by some state legislatures that ban employers from asking employees and/or job applicants for social media passwords. Ford believes that these laws are unnecessary and that the laws undermine an employer's ability to investigate work-related misconduct. The full text of the article is included below.

--

Facebook Password Bills Are Pointless And Unfair

"Facebook password" laws have a surface appeal. Facebook and other social media are ubiquitous — with recent data indicating that roughly half of the U.S. workforce regularly uses some form of social media — so legislators and constituents have a personal interest in keeping employers out of their personal electronic communications.

Yet, it is precisely social media's growing prevalence as a communication tool that makes the overbroad password legislation (which, in most cases, restricts access to publicly available content, not just passwords) so problematic. So when he recently vetoed New Jersey's version of the so-called "Facebook password" bill, Gov. Chris Christie highlighted some of the fundamental flaws in this popular legislation and continued an important conversation about the limits of personal privacy in public forums.

Several states — including Arkansas, Maryland, California, Colorado, Michigan, Illinois, Oregon, Utah, Vermont and Washington — have passed laws to prevent employers from asking job applicants and/or current employees for their social media passwords. These laws seem fairly innocuous and have even drawn an unusual showing of bipartisan support.

Few employers have asked employees or applicants for their passwords, and getting a password via coercion is arguably already prohibited by federal law. Given this, such laws are, at best, pointless and at worst, hamper an employer's legitimate business needs.

Still more troubling is that several of these laws reflect fundamental misunderstandings of how social media sites actually work and, as a result, elevate public communications to private status, with potentially troubling consequences. The Colorado, Maryland, Michigan and Utah statues, for example, prohibit employers from asking for usernames as well as passwords even though, unlike passwords, usernames exist for the specific purpose of publicly identifying the user to others, making a username the least private of all social media information.

Moreover, unlike passwords, usernames are a legitimate and even necessary subject of employer inquiry. Treating a username as "private" could seriously undermine an employer's ability to investigate work-related misconduct and conduct background checks necessary to avoid claims of negligent hiring or negligent retention.

An employer may need to investigate accusations of online bullying or sexual harassment by its employees, for example, as required by state and federal law, yet cannot possibly do so without confirming the usernames of those involved. More fundamentally, employers excluded from identifying an individual's username are prohibited from learning publicly disclosed facts readily available to everyone else.

Overbroad definitions make states' Facebook password laws problematic in other ways. California's law, for example, prohibits an employer from asking an employee to "divulge any personal social media content," regardless, apparently, of whether that social media content comes from the employee's own social media account or something she happened to see on someone else's Facebook page. In the name of "privacy," employers are prohibited from even asking to see public information.

More fundamentally, the definition of what is truly "private" or "personal" in this context raises complex issues related to the nature of the technology and to the complex ways in which that technology is used by employees. It is not always clear who "owns" the information in a particular social media account or whether a particular social media account is personal or business-related.

If the employee creates a Facebook account for his employer, or to promote himself as a spokesperson for the employer, is any of the information posted on that Facebook page personal? Similarly, would information on an employee's LinkedIn account be personal if the employer directed or required that such an account be created in connection with the work?

As courts continue to grapple with these questions, the password protection bills muddy the waters by appearing to treat as private even those accounts that have a direct relationship to the employee's work.

Proponents of the Facebook password laws argue they protect private communications from workplace cyber-snoopers. But that's not the way Facebook and similar sites are actually used. Once again, the legislation appears to be being written largely without reference to the realities of the technology and its users.

Unlike a personal diary, the vast majority of Facebook pages and other social media communications are not kept locked up but are instead readily available to a list of designated "friends" and "friends of friends" who may number in the hundreds or even thousands. Studies suggest that fewer than a third of all Facebook, MySpace, Tumblr and Pinterest users bother to employ the sites' privacy tools to keep their posts from being seen by strangers. Some users would likely point out that the various sites' privacy protections themselves are often complex and not always visible to the user.

But the fact remains that relatively few who use social media take steps to guard their own content. As a result, those posts may be seen by anyone with access to a computer or smartphone — except, in those states that have adopted overbroad privacy bills, by the poster's own employer.

Protecting the privacy of a Facebook page or other social media posting when the user has not taken steps to protect it runs counter to basic principles of privacy law. The common law has long recognized that no right of privacy attaches to any communication in which the individual lacked a reasonable expectation of privacy at the outset.

For most Facebook users, it is not reasonable to expect that communications shared to hundreds of friends — who are then free to instantly share the information with their own friends and friends of friends with or without the original user's permission — could be deemed private in any respect.

In addition, it is not even clear what "access" to "private" information in social media account means. Social media sites like Facebook regularly change the privacy settings on their sites. This means that information that may have been posted with some limited expectation of privacy may lose that expectation thanks not to an affirmative step of the account holder but to a change in the site's privacy protections.

As this has become a relatively common occurrence, once may well argue that no reasonable person should ever have expected, at any time, that anything posted to Facebook or any other social media site could truly be deemed private indefinitely; whether by changing privacy policies or otherwise, all such information was, arguably, always subject to the whims of the social media site's owners and could therefore never have been entitled to any privacy protections in the first place.

Just as most social media users often do not protect the privacy of their online information, some sites are themselves premised entirely on complete openness. Twitter, for example, is based on a model of total disclosure: Unless you take steps to do otherwise, every tweet you post on Twitter is, and is designed to be, seen by virtually anyone, anywhere in the world. As a Manhattan judge observed, "If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy." (*People v. Harris*, New York Criminal Court, June 30, 2012.)

As Christie noted in rejecting the New Jersey password bill, well-intentioned yet overbroad privacy protections can have unintended consequences. Giving social media posts the kind of privacy-plus status that some states' laws have done undermines long-established principles by giving privacy rights to some of the most public forms of communication.