VENABLE® LLP

Labor & Employment News Alert

February 2014

Trojan Horse Privacy Laws: Facebook Snooping

AUTHORS

Todd J. Horn

RELATED PRACTICES

Labor and Employment Litigation

Employee Benefits and Executive Compensation

ARCHIVES

2014 2010 2006
2013 2009 2005
2012 2008 2004
2011 2007

Privacy laws that protect employees at work historically have been considered sparse and virtually toothless. Only employers that engaged in brazen acts of surveillance or intrusion into employees' narrow "zones of privacy" faced liability. While privacy protections have ballooned in the consumer, healthcare, and telecom sectors over the last decade, employee privacy rights largely stood frozen. As a result, businesses paid little attention to workplace privacy compliance obligations. That time has passed.

Like the seemingly benign Trojan Horse in which hid an elite force to attack an unsuspecting enemy, the growing wave of employee privacy laws are far more expansive than they appear on the surface. Indeed, because some of these laws do not even sound like they contain employee privacy protections, they are often ignored. Other privacy laws have "top line" compliance obligations that are easily met, but contain ambiguities and public policy consideration that invite expansive judicial interpretation. One such Trojan Horse privacy law that recently emerged protects employees' social media accounts from employer access.

Employee social media protection laws clearly are in vogue. In the last two years, over half the states have enacted or introduced statutes that generally prohibit employers from requiring employees to disclose passwords to their social media or personal web accounts and protect employees from discipline or termination if they refuse. To the chagrin of multi-state employers, the patchwork of state laws vary widely in scope: some prohibit employers from even "suggesting" that employees disclose their passwords or change their privacy settings; some prohibit unauthorized viewing of private accounts; and some permit requests for account access to investigate theft, harassment, or other workplace misconduct. A common thread of these laws, however, is braided from a public policy view that employees have the right to shield their private on-line activities from their employers' eyes.

As noted above, an employer's "top line" compliance obligations for most password protection laws are straightforward – do not request applicants or employees to disclose their social media passwords unless the applicable statute provides an exception in your circumstances. Remember, however, we are dealing with Trojan Horse privacy laws that contain hidden risks.

One such risk stems from a company's reliance on outdated employee computer monitoring policies. Nearly every private sector employer has a policy notifying employees that they have no expectation of privacy when using company computers, phones, or electronic devices, and that their usage can be monitored at any time, for any reason, without notice. Robust electronic monitoring policies continue to have enormous value, but they are not impenetrable barriers to employee privacy claims. In fact, excessive reliance on an outdated computer monitoring policy can blind your company to the risks posed by the new password protection laws.

Consider a supervisor who is burning to know what his employees are saying about him on their private social media accounts or blogs, which they regularly access on company computers. Armed with an "ironclad" computer monitoring policy, the supervisor logs into his employees' work computers and reviews their web browsing history, including social media activity. How far can the supervisor go under the protection of the computer monitoring policy? If the supervisor limits his review to the actual social media pages the employees accessed on company computers, that is unlikely to generate a viable claim. However, what if the supervisor gains access to the employee's social media account because her work computer saved her password credentials and then snoops around? Under that scenario, the supervisor may be able to see the employee's social media content she ***never viewed*** while she was at work or ***new content*** that she created after she left work.

Another Trojan Horse privacy risk hidden in social media protection statutes can arise with far less effort and by personnel with no authorization to access other employees' computers. Rather than directly asking the "target" employee to turn over his social media password, the supervisor asks a co-worker

"friend" with authorization to view the target employee's account to log in and show the content to the supervisor. Whether this "friend" provides the supervisor with the target employee's private social media content voluntarily, under threat of termination, or completely on his own volition because he dislikes the target employee will impact the liability equation.

Critically, however, under these scenarios the employee's privacy interests in her social media content have been compromised, even though the supervisor never requested or required the employee to provide her password. It does not take a visionary to predict how some courts will view these backdoor tactics to access private employee social media content in light of the underlying policies of the password protection statutes. There is your Trojan Horse.

There is no one-size-fits-all solution to minimize every employer's risk of exposure under the new social media protection statutes. Among the best practices to consider include: analyzing the specific laws and compliance obligations that apply to your organization in light of its locations, size, technology, and culture; designing and implementing clear electronic monitoring, password protection, and **BYOD policies** that consider those factors; blocking employee access to certain sites; and initiating regular training and auditing protocols as the law and technology develop. Employee privacy laws are no longer embryotic; they've grown teeth, and the threat is real.

* * * * *

Todd Horn has over 25 years of experience in employment litigation and compliance initiatives and is the co-author of *Maryland Employment Law*, a treatise that courts cite as a leading reference. Mr. Horn was selected as the "Lawyer of the Year" for employment law in 2011 in Maryland by the publication *Best Lawyers in America*. Mr. Horn also ranks as a top "Band 1" employment lawyer by *Chambers USA*, which reported that he "is admired as a fantastic litigator – one of the best in the courtroom, with a tremendous presence" and "is particularly sought out for high-stakes litigation."