New Laws Protect Social Media Privacy

BY KARL RHODES

Robert Collins, a supply officer with the Maryland Department of Public Safety and Correctional Services, returned to his job in 2010 after taking a leave of absence. While he was gone, the department implemented a policy requiring employees returning from leave to divulge their Facebook user names and passwords as part of background checks to screen out people with gang affiliations. During Collins' recertification process, an interviewer logged on to Collins' Facebook account and browsed through his password-protected postings.

Collins believed the department had invaded his privacy, so he contacted the American Civil Liberties Union. Deborah Jeon, legal director of the ACLU of Maryland, wrote a letter to the agency contending that the policy violated the federal Stored Communications Act. The department voluntarily modified its practices somewhat, but state Sen. Ronald Young introduced legislation to prevent public and private employers in Maryland from requiring employees or job applicants to divulge user names and passwords for personal accounts. (Federal government employers are exempt.) Young also introduced legislation that would block colleges and universities from requiring students or prospective students to provide access to their personal accounts. The schools bill died, but the employer bill passed and took effect in October 2012.

Maryland was the first state in the nation to pass such a law, and Collins' experience has generated much discussion about social media monitoring by employers. Bradley Shear, an attorney in Bethesda, Md., helped Young's staff write the legislation. He says the new law is a "win-win" that protects employees' privacy while shielding employers from liability issues that could arise from social media monitoring.

Erin Egan, Facebook's chief privacy officer, offers the following example: "If an employer sees on Facebook that someone is a member of a protected group (for instance, over a certain age), that employer may open themselves up to claims of discrimination if they don't hire that person." Egan also says that an employer might become liable for failing to protect personal information gleaned from Facebook or for failing to report such information to law enforcement authorities if it suggests criminal activity.

One might assume that employers would prefer to weigh the risks and rewards of social media monitoring without government regulation, but employer advocacy groups have been mostly absent from the public policy discussion over password privacy. "We don't have a formal position on it," says Kate Kennedy, a spokeswoman for the Society for Human Resource Management.

University officials, however, are more open about their social media struggles. The University of North Carolina at Chapel Hill, for example, implemented a monitoring policy partly in response to an NCAA investigation that resulted in serious sanctions against the university's football program. The investigation may have been prompted by tweets by a UNC football player that suggested he may have been receiving gifts from a professional sports agent.

In a public infractions report released in March 2012, the NCAA enforcement staff "alleged a failure to monitor because the institution did not 'consistently' monitor the social networking activity of its student-athletes." The report added that "the social networking site of student-athlete 5 contained information that, if observed, would have alerted the institution to some of the violations."

In 2010, the university started requiring all its student-athletes to allow a coach or an administrator to follow their public posts on Facebook and Twitter, according to Steve Kirschner, UNC's director of sports information. The university has since modified that policy to require student-athletes to register their social media accounts with Varsity Monitor, a contractor that notifies the university when it observes questionable content. Kirschner emphasizes, however, that UNC does not demand access to password-protected content. "We just want to make sure that our student-athletes are representing themselves and their university to the public in appropriate ways," he says.

"It's one thing if it's out there on the Internet for everyone to see," says Shear, the Maryland attorney. But when content is protected from public access, "that's when it should be off limits." Much of Collins' Facebook content, for example, was visible only to people whom he designated.

According to a nationwide survey commissioned by the job-search website CareerBuilder, 37 percent of companies use social networking sites to screen job candidates, and another 11 percent plan to do so. But media reports suggest that only a few employers have required candidates to divulge user names and passwords, and some of those employers say they have abandoned the practice. Even so, three states have passed laws similar to Maryland's, and legislation is pending in 10 additional states. Shear has helped draft a national bill as well. U.S. Representatives Eliot Engel and Jan Schakowsky introduced the Social Networking Online Protection Act (SNOPA) in April 2012.

Collins got his job back with Maryland's Department of Public Safety and Correctional Services, but he left in 2011 to attend nursing school. He understands the importance of screening out people with gang affiliations when hiring correctional officers. But, he adds, "There's a fine line between making sure that the officers are not involved in illicit activity and invading someone's privacy. As officers, we do not forfeit our civil rights." **RF**