Monday, August 1, 2011

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

LegalCURRENTS

Should social media passwords be a job requirement?

I recently learned that the Yates County Sheriff's Department was requiring current employees and job applicants to provide the department with their social media passwords. The requirement was later rescinded for current employees.

By NICOLE BLACK
Daily Record Columnist

The Yates County Sheriff's Department isn't alone. Requiring social media passwords as part of the job application process is an increasing trend — and a disturbing one, especially when the employer is a governmental entity, such as a law enforcement agency.

A similar case made the news earlier this year when Maryland corrections officers were required to provide the Maryland Division of Corrections access to their Facebook accounts as part of the job recertification process.

The ACLU of Maryland became involved and challenged the policy, asserting that the policy violated the privacy right of employees, job applicants and their "friends" on social networks. In January, the ACLU sent a letter to the DOC (www.aclu-md.org) summarizing its objections. In part, the ACLU objected to the privacy violations occurring because of the policy:

"Neither Officer Collins nor his Facebook 'friends' deserve to have the government snooping about their private electronic communications. Login information gives the DOC access to communications that are intended to be private … [and] the DOC demand for login information is equivalent to demands that they produce all of their private correspondence and photographs for review, or permit the government to listen in on their personal telephone calls, as a condition of employment."

The Maryland DOC later suspended the policy for 45 days as it related to current employees and in April revised the social media policy somewhat, but the revisions did little to alleviate the ACLU's privacy concerns.

The Maryland DOC and the Yates County Sheriff's Department aren't the only law enforcement agencies requiring applicants to provide social media passwords. In fact, according to a November 2010 report, the IACP Social Media Survey, issued by the International Association of Chiefs of Police, nearly one third of all law enforcement agencies required access applicants to provide access to their social media profiles as part of the background check.

That so many law enforcement agencies engage in this practice is troubling for any number of reasons. Many social media users choose to limit public access to their social media profiles in order to enhance their levels of privacy and they do so for a reason: to keep their personal information private. When an agency obtains passwords to an applicant's social media profiles, the agency is able to access all electronic communications related to the profiles, regardless of the privacy settings in place.

Additionally, when agencies obtain passwords to these profiles, they gain access to a vast array of information, including communications from unsuspecting third parties. These communications include messages and photographs posted to the applicant's wall, status messages from friends that appear in the applicant's social media stream and private messages from other users that are intended for the applicant's eyes only.

Even if law enforcement job applicants consent to allow hiring agencies access to social media profile passwords, the "friends" of the applicants most certainly did not consent to having communications that they believed to be private perused by law enforcement officials.

Thus, policies of this type infringe upon the privacy rights of innocent, unsuspecting third parties who happen to be friends with and correspond with job applicants. For that reason alone, this practice should be terminated.

Nicole Black is of counsel to Fiandach & Fiandach in Rochester. She co-authors the ABA book Social Media for Lawyers: the Next Frontier, and co-authors Criminal Law in New York, a West-Thomson treatise, She is the founder of lawtechTalk.com and speaks regularly at conferences regarding the intersection of law and technology. She publishes four legal blogs and can be reached at nblack@nicoleblackesq.com.