

MARCH 6, 2013 | BY DAVE MAASS

States Seek Ban to Employers' Social-Media Snooping

When EFF considers a job applicant, we ask for the usual information: a resume, references, maybe writing samples. When we decide to hire someone, we require a few more pieces of personal data, the standard HR stuff, to ensure the lucky employee gets paid on time and is covered by health insurance.

What doesn't EFF demand? Social media passwords.

We don't require applicants to unlock their Facebook accounts and reveal their private communications, photo albums or calendars. No one here demands the potential employees unlock their Twitter or Google+ accounts to expose their private, direct messages. We certainly don't want to know what they're posting about themselves on online dating sites or on closed Bible study messageboards.

This isn't only because EFF respects its employees' privacy. It's because, as of Jan. 1, it's the law in California.

Last year, Maryland became the first state to explicitly prohibit employers from forcing applicants or workers to disclose their personal names or passwords as a condition of employment. California followed soon after with its own measure, which further bars private employers from even requesting access to their workers social-media accounts. According to the National Conference of State Legislatures, **some 28 states** are weighing legislation addressing the issue in one regard or another in 2013.

Broadly speaking, an individual should not have to open up their online private lives to get or keep a job. Not only is it an invasion of the job-seeker's privacy, but such practices expose personal information belonging to friends and family members who thought they were communicating privately within a closed network.

Think of it another way: You wouldn't want to hand the keys to your apartment to a

potential employer and let them rummage through your cupboards, pick through your diary and sit in the corner during your dinner parties. And, even if you were open to that, you'd probably have some pretty irritated houseguests and roommates.

The legislative proposals across the country vary. In one case brought to our attention by the [Columbus Dispatch](#), the state senate in Ohio began hearings last week on legislation that includes a peculiar twist.

The language in [SB 45](#) only bans employers from “recklessly” demanding applicants provide access to their social media accounts. On one hand, it's encouraging that the Ohio legislature is looking at the issue, but we're curious why the authors would only ban reckless privacy invasion rather than propose an across-the-board ban on the practice. After all, that kind of qualifier is fairly subjective; what we might consider abuse in regards to privacy, a company might deem responsible to its corporate mandate.

While Ohio seeks limited reforms, California is seeking to expand its ban this session to cover public entities, including law enforcement agencies. The bill, [AB 25](#), raises some fascinating questions, especially with regard to civil liberties.

According to [U-T San Diego](#), local law-enforcement agencies require recruits to sit down with an officer and open their Facebook accounts. Although the agencies already run applicants through rigorous background checks, recruiters claim a social-media inspection is one more way to “weed out weak links,” as the columnist put it.

A citizen's gut reaction might be, “OK, sure, we do want to know what potential cops are saying on Facebook.” But imagine this scenario: A Facebook friend of yours is applying to be a deputy and gives the recruiter the password to his account. Suddenly, a law enforcement agency has access to your private posts—the ones that would only show up in your friend's feed or mailbox—without anything remotely resembling a warrant and certainly not your consent.

In an economy where jobs are scarce, an unemployed individual is under significant pressure to yield to whatever requirements an employer might set, no matter how invasive. This is just another way concepts of privacy are under attack

in the digital age and, as always, a social media user needs to consider that what they post online might not be as confidential as they assume. Employers are frequently using search engines to vet recruits and so it's important to be aware of your privacy settings on sites such as Facebook (here's [one guide](#) to locking down your account).

If you're an employee or looking for a job, it can help to become familiar with your state laws as well as the social-media policies for the companies where you're applying. The Privacy Rights Clearinghouse has a comprehensive [fact sheet on social media privacy](#) that covers these issues, as well as [resources](#) to help you understand the pitfalls and limits to background checks. [ComplianceBuilding.com](#) has a running spreadsheet of social-media policies enacted by more than 230 large employers.

Fortunately, in some states you do have rights and in other states you will have rights soon. That is, if the forces of privacy prevail. While a step in the right direction, legislators could do a lot more to protect and employer employees in a digital age.

Privacy

Social Networks