USA TODAY™ 07.09.14
A GANNETT COMPANY

Password protected: States pass anti-snooping laws

Jeffrey Stinson, Pew/Stateline Staff Writer *10:43 a.m. EDT July 8, 2014*

(Photo: Matt Rourke, AP)

Worried about your boss prying into your personal business, poking around in aspects of your life you'd rather keep between friends and family — even as you're sharing more of it on social media?

Seventeen states have drawn a line on what's your business and what your boss can access by passing laws that ban employers from asking for the logins and passwords to the personal social media, email and other online networking accounts of their workers and prospective hires.

Since Maryland passed the first ban two years ago after a state employee complained of having to reveal the password to his Facebook account, legislatures in states as politically different as Michigan and California, New Jersey and Utah, have passed laws that impose restrictions on snooping by government and private employers.

Louisiana, Oklahoma, Tennessee and Wisconsin passed laws this year, while Maine lawmakers voted to study restrictions. Similar legislation was introduced this year or is pending in more than 20 other states, according to tracking (http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014) by the National Conference of State Legislatures.

As social media explodes in popularity, employers increasingly are concerned that what employees say in cyberspace could damage their business. Meanwhile, more workers are bringing their own smartphones and tablets into the office.

Sponsors of the legislation say the laws are needed to keep basic privacy rights apace with technology.

"Fifty years ago, if somebody brought in a stack of personal correspondence and put it in their locker, the employer wouldn't demand to see it," said Republican state Sen. Kyle Loveless, Senate sponsor of Oklahoma's law, which was signed in May. "In today's time, people put (personal correspondence) online. An employer shouldn't have the right to see it.

"I'm an employer, and as an employer I shouldn't have the right to demand that of an employee or a prospective employee," said Loveless, who operates a family orthopedic footwear business in Oklahoma City.

Like several states, Wisconsin's law also prohibits college and school administrators, coaches and teachers from demanding access to students' personal accounts.

Even many elementary school students now have smartphones loaded with personal information, said state Rep. Melissa Sargent, a Democrat from Madison who sponsored the law in the Wisconsin Assembly.

A smartphone today, she said, is "akin to a scrapbook" in which previous generations kept baby pictures and postcards from grandparents. "Do you bring a scrapbook to a job interview? Do you bring it to school and let everyone see it?"

'Mortified'

A case that helped initiate the flurry of laws was that of Robert Collins, a Maryland correctional supply officer who sought to return to work after taking family leave in 2010.

Collins told the Maryland House Economic Matters Committee two years ago that he was "mortified" when a hiring investigator asked to log into his Facebook account as part of his reinstatement interview. The investigator said he was concerned about any gang connections.

"I said, 'you can't be serious,'" Collins testified. "He said, 'I am as serious as a heart attack.' I did not want to do it, but because I really needed my job and he implied that this was a condition of recertification, I reluctantly gave him my password."

Like the 2012 Maryland law, other laws generally apply to state and local government, as well as private-sector employers. Most apply to accessing the personal accounts of job seekers, as well as employees. Like Wisconsin, many states also include colleges, where coaches seek to control what athletes say. Arkansas and Delaware aim their laws at colleges.

Many states prohibit retaliation against employees who refuse to surrender their passwords. Some [illegible] se fines ranging from $500 to $1,000 for violations.

The laws reflect growing privacy concerns even as people are ramping up use of social media such as Facebook, which had about 160 million daily users in the U.S. and Canada in March, or Twitter, whose users send out an average of 115 million tweets a day in the U.S.

Some 73% of American adults who go online now use social media, a December survey (http://www.pewinternet.org/2013/12/30/social-media-update-2013/) by the Pew Research Center's Internet Project found. And 42% said they use more than one social networking site.

At the same time, 11% of Internet users say they've tried to hide their online activity from an employer, supervisor or co-workers, another Pew Research survey (http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/) found in September. Nearly 70% said it was very important that only they or those they authorized had access to their emails. (*Stateline* is also funded by Pew.)

"I think this is a visceral reaction," Allie Bohm, advocacy and policy strategist for the American Civil Liberties Union, said of the flurry of state laws. "Privacy in the digital age is an incredibly hot topic."

Whether the laws are justified by widespread abuse isn't clear. Loveless, who sponsored the Oklahoma law, and Sargent, the Wisconsin sponsor, said they had known of instances when employers asked for passwords.

But the nonprofit Privacy Rights Clearing House (https://www.privacyrights.org/), which collects citizen complaints of abuse, had none involving employers demanding social media passwords over the last two years. Executive Director Paul Stephens said states are passing the laws because the federal government hasn't been aggressive enough in protecting privacy as concerns have arisen.

Littler Mendelson, the nation's biggest labor and employment law firm, found only 1% of the 417 business respondents it surveyed (http://www.littler.com/files/press/related-files/2013-Executive-Employer-Survey-Report.pdf) last year asked for social media logins as part of hiring.

Employers' concerns

Bosses have related protections under the laws. Employers can access accounts on devices that they provide employees and, in many instances, if employees are using employer-provided access to the Internet.

Some laws spell out that employees cannot divulge private company or government information that they have access to on the job. Others, like Oklahoma's, don't. But Loveless said, "If it's illegal to do before social media, it's illegal now."

Employers' concerns are legitimate as are their requests to access personal accounts, said Nancy Flynn, founder of the ePolicy Institute (http://www.epolicyinstitute.com/index.asp) that advises employers on policy in the digital age. The financial, legal and competitive stakes are high if certain company information becomes public, she said.

"They're trying to protect their organization," she said. "They're not just trying to snoop around and look at embarrassing photos. They are trying to protect their company, their customers, their investors."

As the laws have proliferated so has the practice of more workers taking their own mobile devices to work. And more employers are establishing policies on what employees cannot say about their work online, publicly and privately, on personal as well as employer-provided devices.

The lines can blur between an employer's and personal devices. A survey of 447 human resources professionals earlier this year found 42% of employers subsidized employees' personal phones if they used them for business. And 41% offered a business phone for personal use, the survey (http://www.shrm.org/Research/SurveyFindings/Documents/14-0301%20Benefits_Report_TEXT_FNL.pdf) by the Society for Human Resource Management found.

In Minneapolis, the city lets its employees use their own smartphones, laptops and tablets on the job when they choose. While there's no laundry list of rules on their use, employees are expected to follow city policy on what information isn't to be made public, whether on city-owned devices or not.

"We trust people as professionals," said Otto Doll, the city's chief information officer and former chief information officer for South Dakota. "We say, 'We expect you to abide by the rules.'" The city doesn't demand passwords to its employees' online accounts, although the state of Minnesota doesn't have a law forbidding it. Nor does it monitor employees' activity, Doll said, only network security.

"We're not the CIA or NSA," Doll said. "It boils down to people, their attitudes and their actions. We start with the position they're professionals and will do the right thing."