THE NATIONAL LAW JOURNAL
ALM Properties, Inc.
Page printed from: *http://www.nlj.com*

Invasions of privacy

Congress and state legislatures are properly barring employers' demands for social-media passwords.

Lynne Bernabei and Alan R. Kabat
July 23, 2012

Most people think Facebook or LinkedIn passwords are confidential. But employers do not always agree. Increasingly, employers are asking for employees' or job applicants' social-network passwords, which is a hard request to refuse. In a pushback against invasions of privacy, Congress and state legislatures are proposing and passing legislation to prevent the invasion of personal social-network sites by employers and potential employers.

Why should it be illegal for employers and universities to review the private content of social-media Web sites? Because employment and educational decisions can be tainted by knowledge of a person's protected status, particularly for applicants. An employer or school may not know an applicant's age, race, religion, disability or sexual orientation unless they are able to examine the private information on a social-media Web site. Current employees or students may not want their employers to know about interracial dating habits, religious or political beliefs, or support for diversity. The National Labor Relations Board has held that employers — even in nonunionized workplaces — may not discipline employees who use social-media to discuss or protest workplace issues. For government employees, their social-media Web sites may have First Amendment protected speech, which cannot form the basis for discipline.

Thus, Congress and 12 state legislatures have proposed legislation to prevent employers and schools from making decisions based on the private content of Web sites. These legislative efforts were prompted by controversies caused by several governments that required applicants and employees to disclose nonpublic social-media information. For example, the city of Bozeman, Mont., required applicants' passwords, and only stopped after a media firestorm in 2009. In Illinois and Virginia, some county sheriffs required applicants to "friend" the sheriffs, so they could check private Web sites.

Two years later, the American Civil Liberties Union protested when the Maryland Department of Public Safety and Correctional Services required a corrections officer to provide his Facebook user name and password during a recertification interview. The corrections officer saw the interviewer logging into his Facebook account, and reviewing his private messages. The state agency claimed it had to ensure that corrections officers did not have ties to gang members. In 2012, the Maryland Legislature quickly passed what became the first law prohibiting employers

from requiring or demanding employees and applicants to disclose their user names or passwords.

Some colleges required student-athletes to disclose social-media passwords to coaches or campus compliance officers, ostensibly to comply with National Collegiate Athletic Association ethics requirements. Indeed, two companies now market "monitoring" services to colleges. However, the NCAA stated in March that while monitoring of publicly accessible social-media Web sites was permissible, colleges were not obligated to monitor the private content of athletes' Web sites.

Congress and other states have jumped on the bandwagon. Other pending legislative efforts include Illinois legislation, recently approved by both chambers and awaiting the governor's review and approval, barring employers from demanding these passwords. Legislation is still pending in committees in the U.S. Congress, California, Delaware, Maryland (for educational institutions), Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, South Carolina and Washington. Senators Richard Blumenthal (D-Conn.) and Charles Schumer (D-N.Y.) also requested that the Equal Employment Opportunity Commission and the Department of Justice investigate whether employers' coercive demands violate federal computer statutes that prohibit unauthorized access, or violate the anti-discrimination laws.

The good news is that this legislation prohibits employers or schools from requiring employees, students or applicants to disclose their social-media passwords, or otherwise to provide access to private material on social-media Web sites. These legislative efforts also prohibit taking adverse actions against individuals who refuse to disclose their passwords.

Delaware has gone further. Its proposed legislation prohibits employers from requiring "shoulder surfing," through which the employee would have to log onto the social-media account in the employer's presence, and allow a manager to view the private content. The proposed Delaware law also would prohibit employers from using another person to access a social-media Web site. For example, if a hiring manager knew that an employee is a Facebook friend of an applicant, the hiring manager could not direct that employee to report to the hiring manager on the private content of the applicant's Web site. Delaware also would prohibit an employer from requiring an employee or an applicant to "friend" a supervisor or hiring official, so that the employer could directly access the private content of the employee's or applicant's site.

The bad news is that these legislative efforts have a hodgepodge of enforcement mechanisms. For example, there are five bills pending in New York, two of which have both civil and administrative remedies, one of which has an administrative remedy alone and two of which have no statutory remedies. Michigan's and Washington's bills provide for a civil action for legal and equitable remedies; Michigan's also would create a misdemeanor offense punishable by up to 93 days in jail. New Jersey's and Ohio's bills provide both administrative enforcement and a civil action. Delaware and Illinois drafted their legislation as part of pre-existing statutes with enforcement mechanisms through both a state agency and a civil action.

The congressional legislation has particularly complex enforcement provisions that may be of little use. H.R. 5050, the "Social Networking Online Protection Act," allows for enforcement

only through the U.S. Department of Labor, at a time when that agency lacks the resources to enforce other federal employment statutes. H.R. 5684, "Password Protection Act of 2012," would be added to the Computer Fraud and Abuse Act, 18 U.S.C. 1030, a complex statute with mixed criminal and civil enforcement components, under which employees may have a difficult time enforcing their rights.

Other states did not include any enforcement mechanism in their legislation. These include California, Maryland, Minnesota, Missouri, New York (two bills) and South Carolina. However, employees in those states may be able to bring a common law tort claim for wrongful discharge in violation of public policy, by using the legislation as a source of the public policy.

There are also problematic scienter requirements. Ohio's proposed legislation prohibits employers from "recklessly" asking or requiring applicants or employees to provide user names or passwords. Requiring an employee to prove the employer's motivation might be a difficult or impossible task.

The federal Password Protection Act of 2012 would allow employers to fire or discipline employees if their refusal to disclose their password "is not a motivating factor for the discharge or discipline of the individual." Employment litigators already have to deal with an inconsistent patchwork of causation factors under the federal statutes — e.g., "but-for" causation, "sole" cause, "motivating factor" and "contributing factor." The scienter requirement in this proposed legislation simply creates more problems, given that "motivating factor" has been interpreted in different ways under other federal employment statutes, leading to different results.

In addition, some legislative efforts have a hodgepodge of exemptions. Delaware's proposed legislation exempts law enforcement agencies — precisely the employment sector that motivated Maryland's legislation. It also proposes to exempt "employers in the financial services industry…[in] conducting internal investigations into employee wrongdoing, complying with the supervision requirements of the [Securities and Exchange Commission, Financial Industry Regulatory Authority] or other financial regulators, or achieving waver [sic] of the personal communications protections in employment contracts." This loophole is big enough to drive a truck through, since the financial sector is one of the largest employers in Delaware, and almost anything can be an "internal investigation."

The federal Password Protection Act of 2012 would allow executive-branch agencies to exempt positions "requiring eligibility for access to classified information." Since more than 4.2 million federal employees and contractors have security clearances, this means that numerous individuals could be required to disclose their private information in order to keep their jobs.

Congress and a number of state legislatures are attempting to solve the problem of employers and schools improperly demanding access to private, password-protected content of social-media Web sites, but are enacting legislation that may lead to complex litigation over privacy rights.

Lynne Bernabei and Alan R. Kabat are partners at Bernabei & Wachtel in Washington, where they represent whistleblowers and other employees.