F I S C A L I M P A C T R E P O R T

SPONSOR Candelaria **ORIGINAL DATE** 02/13/13 02/26/13 **LAST UPDATED** 03/01/13 **HB**

SHORT TITLE No Social Media Access for Employers **SB** 371/aSJC/aSFl#1

ANALYST Daly

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY13	FY14	FY15	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total	NFI	NFI	NFI			

(Parenthesis ( ) Indicate Expenditure Decreases)

SOURCES OF INFORMATION
LFC Files

Responses Received From
Attorney General's Office (AGO)
State Personnel Office (SPO)
Workforce Solutions Department (WSD)

SUMMARY

Synopsis of SFL Amendment #1

The Senate Floor Amendment #1 to Senate Bill 371 strikes the phrase "or other related account information" so the statement reads: It is unlawful for an employer to request or require a prospective employee to provide a password…."

Synopsis of SJC Amendment

The Senate Judiciary Committee amendment to Senate Bill 371 consolidates and clarifies the bill's language recognizing the employer's right to have in place policies regarding work place internet use, social networking site use and electronic mail use.

Synopsis of Original Bill

Senate Bill 371 (SB 371) prohibits employers from requesting or requiring a prospective employee to provide a password or access to the prospective employee's social networking account. The bill does not limit an employer's right to: (1) promulgate and maintain lawful

workplace policies; (2) govern the use of the employer's electronic equipment; (3) have policies regarding internet use, social networking site use and electronic mail use; and (4) monitor usage of the employer's electronic equipment and the employer's electronic mail. The bill does not prohibit an employer from obtaining information about a prospective employee that is in the public domain.

FISCAL IMPLICATIONS

No fiscal implication is anticipated, particularly in light of the absence of any penalty or other enforcement mechanism.

SIGNIFICANT ISSUES

The Attorney General's Office (AGO) advises that privacy in social networking:

> is an emerging, but underdeveloped, area of case law. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 872 F. Supp. 2d 369, 373 (U.S.D.Ct. N.J. 2012). There appears to be some consistency in the case law on the two ends of the privacy spectrum. On one end of the spectrum, there are cases holding that there is no reasonable expectation of privacy for material posted to an unprotected website that anyone can view. *Id.* On the other end of the spectrum, there are cases holding that there is a reasonable expectation of privacy for individual, password-protected online communications. *Id.* Courts, however, have not yet developed a coherent approach to communications falling between these two extremes.

However, the Workforce Solutions Department (WSD) warns that compelling employee passwords or access, which is the practice being prohibited in SB 37:

> may potentially subject the employer to civil liability under federal laws, including the Stored Communications Act (SCA) or the Computer Fraud and Abuse Act (CFAA). These two acts prohibit intentional access to electronic information or to a computer without authorization. Two courts have found that when supervisors request employee login credentials, and use them to access otherwise private information they may be subject to civil liability under the SCA. *Pietrylo v. Hillstone Restaurant Group*, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009); *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001).

Every agency commenting on this bill have called attention to the absence of any enforcement or penalty provisions in the event the behavior being declared unlawful occurs. The WSD notes that SB 371 does not authorize the Human Rights Bureau or the Human Rights Commission to investigate or hear cases involving alleged violations of the bill. Absent such grants of authority or other enforcement mechanisms or penalties, it is unclear what recourse a prospective employee may have against a potential employer who violates SB 371.

The State Personnel Office (SPO) raises concern about the lack of definitions for "employer" and "prospective employee", particularly since there are no exceptions for high security or safety sensitive positions. Similarly, there is no exception for appointed positions. As to the state, the SPO warns this could lead to potential liability for lack of due diligence in conducting background checks for certain positions, and might also impact the vetting process for positions

which are appointed by the governor.

Similarly, the SPO points to other terms that are not defined that it suggests may lead to confusion as to what is prohibited:

> Section 1(A) makes it unlawful for an employer to demand access in any manner to the prospective employee's account or profile. As "demand access" is not defined, it is unclear if this would also apply to an employer navigating on their own on the website, attempting to gain access. Also, it is unclear if asking a prospective employee whether or not they even have an account on a particular social networking website would be considered "related account information" and thus prohibited.
>
> There is also a conflict between subsections C and D(1). Subsection C provides that the statute will not apply to an employer gaining information from the public domain. However, "public domain" is not defined. Subsection D(1) includes "public profile" within the definition of "social networking website". However, "public profile" is not defined either. Is a "public profile" on Facebook (for example) considered public domain if the employer does not have its own Facebook account? What if the employer does have its own Facebook account and thus the capability to search Facebook and view public profiles? The lack of definitions could lead to confusion as to what an employer can and cannot ask or search for during the screening and evaluation of a prospective employee.
>
> Subsection D defines "social networking site". Part of that definition is a "bounded system" created by an internet based service. "Bounded system" is not defined. This lack of definition, again, could lead to confusion and litigation as to which websites qualify under the proposed statute. Is it a system requiring membership or a password? Is it more akin to an intranet, accessible solely within a particular organization?

OTHER SUBSTANTIVE ISSUES

According to the National Conference of State Legislatures, four states--California, Illinois, Maryland and Michigan--enacted legislation in 2012 that prohibits employers requesting or requiring a prospective employee or applicant to disclose a user name or password for a personal social media account. Ten other states introduced similar legislation last year, and legislation on this topic has been introduced or pending in at least 26 states (including New Mexico) in 2013.

The four enacted laws use many of the same terms contained in SB 371 without further definition. Only one of those laws contains any penalty or other enforcement mechanism: Michigan's statute makes a violation a misdemeanor punishable by a fine of not more than $1,000. It also authorizes a person subject of a violation of that law to bring a civil action seeking injunctive relief and damages of not more than $1,000, plus reasonable attorney fees and court costs.

MD/svb:blm