

---

---

## **OLR Bill Analysis**

### **sSB 317**

#### ***AN ACT CONCERNING EMPLOYEE PRIVACY.***

##### **SUMMARY:**

This bill prohibits employers from requesting or requiring an employee or job applicant to (1) provide the employer with a user name, password, or other way to access the employee's or applicant's personal online account or (2) access such an account in front of the employer. It also bars employers from (1) firing, disciplining, or otherwise retaliating against an employee who refuses to provide this access or (2) refusing to hire an applicant because the applicant would not provide access to his or her personal online account.

The bill makes exceptions for accounts and devices the employer provides and for certain types of investigations. It does not apply to any state or local law enforcement agency conducting a preemployment investigation or review of law enforcement personnel.

It allows employees and applicants to file a complaint with the labor commissioner, who can impose civil penalties of up to \$25 for initial violations against job applicants and \$500 for initial violations against employees. Penalties for subsequent violations can be up to \$500 for violations against applicants and up to \$1,000 for violations against employees.

EFFECTIVE DATE: October 1, 2014

##### **BAN ON REQUESTING ACCOUNT ACCESS**

The bill bans an employer from requesting or requiring an employee or job applicant to (1) provide the employer with a user name, password, or any other authentication needed to access a personal online account or (2) authenticate or access the account in the employer's presence. Employers covered by the bill include the state

and its political subdivisions, but not state or municipal law enforcement agencies conducting preemployment investigations or reviews of law enforcement personnel.

Under the bill, a “personal online account” is an online account the employee or applicant uses exclusively for personal purposes unrelated to any of the employer’s business purposes, including e-mail, social media, and retail-based Internet web sites. It does not include any account created, maintained, used, or accessed by an employee or applicant for the employer’s business purposes.

### **BANS ON RETALIATION**

The bill bans employers from discharging, disciplining, discriminating against, retaliating against, or otherwise penalizing an employee who:

1. refuses to provide the employer with a user name, password, or any other authentication for accessing his or her personal online account;
2. refuses to authenticate or access an account in front of the employer; or
3. files, or causes to be filed, any verbal or written complaint with a public or private body or court about the employer’s request for access to a personal account or retaliation for refusing such access.

It also prohibits employers from failing or refusing to hire an applicant because he or she would not (1) provide a user name, password, or any other authentication for accessing his or her personal online account or (2) authenticate or access an account in the employer’s presence.

### **EXCEPTIONS**

The bill provides a number of circumstances under which an employer can request or require an employee or applicant to provide a user name, password, or other authentication means for a personal

online account.

### ***Employer's Accounts and Devices***

It allows an employer to request or require that an employee or applicant provide access to:

1. any account or service (a) provided by the employer or by virtue of the employee's work relationship with the employer or (b) that the employee uses for business purposes or
2. any electronic communications device the employer supplied or paid for, in whole or in part.

It defines "electronic communications device" as any electronic device capable of transmitting, accepting, or processing data, including a computer, computer network and computer system, as defined in state law, and a cellular or wireless telephone.

### ***Investigations***

The bill allows exceptions for certain investigations, with limitations. Employers can conduct an investigation:

1. to ensure compliance with (a) applicable state or federal laws, (b) regulatory requirements, or (c) prohibitions against work-related employee misconduct based on receiving specific information about activity on an employee or applicant's personal online account or
2. based on receiving specific information about an employee or applicant's unauthorized transfer of the employer's proprietary information, confidential information, or financial data to or from a personal online account operated by an employee, applicant, or other source.

An employer conducting these investigations can require an employee to provide access to a personal online account, but cannot require disclosure of the user name, password, or other means of accessing the personal online account.

The bill permits an employer to discharge, discipline, or otherwise penalize an employee or applicant who transferred, without the employer's permission, the employer's proprietary information, confidential information, or financial data to or from the employee or applicant's personal online account.

### ***Monitoring and Blocking Data***

The bill allows an employer to monitor, review, access, or block electronic data stored on an electronic communications device paid for in whole or in part by the employer or traveling through or stored on an employer's network, in compliance with state and federal law.

### ***State and Federal Laws***

The bill specifies that it does not prevent an employer from complying with state or federal laws, regulations, or rules for self-regulatory organizations (e.g., businesses regulated by the Securities Exchange Commission's rules).

## **ENFORCEMENT**

The bill allows any employee or applicant to file a complaint with the labor commissioner alleging an employer requested or required access to a personal online account or retaliated for a refusal to provide access. The commissioner must investigate a complaint and may hold a hearing, after which she must send each party a written decision. Any employee or applicant who prevails in a hearing must be awarded reasonable attorney's fee and costs.

If the commissioner finds an employer violated the bill's ban on requesting access to an employee's account, or retaliated against an employee for refusing to provide access, she can (1) levy a civil penalty against the employer of up to \$500 for an initial violation and \$1,000 for each subsequent violation and (2) award the employee all appropriate relief, including rehiring or reinstatement, back pay, reestablishment of wages, or any other relief the commissioner deems appropriate.

If she finds an employer violated the bill's ban on requesting access

to an applicant's account, or refused to hire an applicant for refusing to provide access, she can (1) levy a civil penalty against the employer for up to \$25 for an initial violation and \$500 for each subsequent violation.

The commissioner may ask the attorney general to bring a civil suit to recover any of the above civil penalties. Any party aggrieved by the commissioner's decision may appeal to the Superior Court.

**COMMITTEE ACTION**

Labor and Public Employees Committee

Joint Favorable Substitute

Yea 8 Nay 2 (03/18/2014)