

SENATE BILL REPORT

SSB 5211

As Amended by House, April 17, 2013

Title: An act relating to social networking accounts and profiles.

Brief Description: Concerning social networking accounts and profiles.

Sponsors: Senate Committee on Commerce & Labor (originally sponsored by Senators Hobbs, Eide, Kline, Ranker, Hatfield, Harper, Billig, Hasegawa, Kohl-Welles, Shin, Keiser, Frockt, Rolfes, Hill, Conway and Nelson).

Brief History:

Committee Activity: Commerce & Labor: 2/18/13, 2/22/13 [DPS].

Passed Senate: 3/13/13, 49-0.

Passed House: 4/17/13, 97-0.

SENATE COMMITTEE ON COMMERCE & LABOR

Majority Report: That Substitute Senate Bill No. 5211 be substituted therefor, and the substitute bill do pass.

Signed by Senators Holmquist Newbry, Chair; Braun, Vice Chair; Conway, Ranking Member; Hasegawa, Hewitt, Keiser and King.

Staff: Mac Nicholson (786-7445)

Background: State law does not prohibit an employer from requiring an employee or prospective employee to submit social media passwords or other account information as a condition of employment or continued employment.

Summary of Substitute Bill: An employer cannot require, as a condition of employment, any employee or prospective employee to submit any password or other related account information in order to gain access to the individual's personal social networking website account or profile.

A social media networking website is an internet-based service that allows individuals to construct public or semipublic profiles within a system; create a list of other users with whom they share a connection; and view or navigate their list of connections and those made by others within the system.

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

An employer may obtain information about an employee or prospective employee that is in the public domain or that is otherwise obtained in compliance with the legislation.

The legislation does not prevent an employer from complying with the requirements of state or federal statutes, rules or regulations, case law, or rules of self-regulatory organizations.

An employee may bring a civil action alleging a violation of the legislation. The court may award a prevailing employee statutory damages of \$500, actual damages, and reasonable attorneys' fees and costs. If the court finds the action was frivolous and advanced without reasonable cause, the court may award reasonable expenses and attorneys' fees to the employer.

Appropriation: None.

Fiscal Note: Not requested.

Committee/Commission/Task Force Created: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony on Original Bill: PRO: This bill is driven from news articles about employers asking employees for Facebook passwords. Other states have passed similar laws, and while it is not prevalent in Washington State yet, social media use is growing and it is a good idea to do this now.

CON: This is a complex issue, and it is not clear if certain social network programs do not meet the definition in the bill. It is going to take some time to get the bill ready and to come up with necessary exemptions, such as emergency situations and trade secrets.

OTHER: There is a concern about employers having access to passwords for company accounts maintained by an employee. Under federal security laws, there is an obligation to monitor the social network activity of employees so personal and business financial activities do not blend. Exemption language used in other states should be incorporated into this bill as well.

Persons Testifying: PRO: Senator Hobbs, prime sponsor.

CON: Michael Shaw, WA State Bar Assn.

OTHER: Patrick Connor, National Federation of Independent Business; Bill Stauffacher, Securities Industry and Financial University Place Markets Assn.

House Amendment(s): The House amendment provides additional language regarding the prohibition on requiring submission of a social network password or other related account information in order to gain access to the personal account or profile. The new language prohibits an employer from:

- requesting, requiring, or otherwise coercing an employee or applicant to: (1) disclose login information for personal social networking accounts; or (2) access their account in

the employer's presence in a manner that enables the employer to observe the contents of the account;

- compelling or coercing an employee or applicant to add a person to the list of contacts associated with the account;
- requesting, requiring, or otherwise causing an employee or applicant to alter the settings on the account that affect a third party's ability to view the contents of the account; or
- taking adverse action against an employee or applicant for refusal to provide login information, access the account in the employer's presence, add a person to contacts lists, or alter the account settings.

The House amendment provides employers the ability to require an employee to share content from personal social networking accounts if:

- the employer requests or requires the content to make a factual determination in the course of an investigation;
- the investigation is undertaken in response to receipt of information about the employee's activity on personal social networking accounts;
- the purpose of the investigation is either: (1) to ensure compliance with laws, regulatory requirements, or prohibitions against work-related employee misconduct; or (2) to investigate an allegation of unauthorized transfer of the employer's proprietary information, confidential information, or financial data; and
- the employer does not request or require the employee to provide login information.

The House amendment provides additional exemptions so that the bill does not:

- apply to a social network, intranet, or other technology platform intended primarily to facilitate work-related information exchange, collaboration, or communication;
- prohibit an employer from requesting or requiring an employee to disclose login information for access to an account or service provided by virtue of the employment relationship or to an electronic communications device or online account paid for or supplied by the employer;
- prohibit an employer from enforcing existing personnel policies that do not conflict with the bill; or
- prevent an employer from complying with requirements of statutes, rules, case law, or rules of self-regulatory organizations.

The House amendment changes the enforcement mechanism. Instead of a private lawsuit, an employee or applicant may file a complaint with the Department of Labor and Industries (L&I), who must then investigate the complaint and hold a hearing in accordance with the Administrative Procedures Act. A finding pursuant to this procedure constitutes an exhaustion of administrative remedies. L&I is given rule-making authority, and a penalty established in rule may not exceed \$1,000 for the first violation and \$5,000 for subsequent violations.

If an employer inadvertently receives login information through use of an employer-provided electronic communications device or an electronic device or program that monitors an employer's network, the employer is not liable for possessing the information but may not use it to access the employee's account.

The House amendment appropriates \$23,064 to L&I for the fiscal year ending June 30, 2014, and provides an immediate effective date.