SUBJECT: Prohibiting employers from accessing employees' personal online accounts

COMMITTEE: Business and Industry — committee substitute recommended

VOTE: 7 ayes — Oliveira, Bohac, Orr, E. Rodriguez, Villalba, Walle, Workman

0 nays

WITNESSES: For — Rick Levy, AFL-CIO

Against — Cathy Dewitt, Texas Association of Businesses; John Fleming, Texas Mortgage Bankers Association; Karen Neeley, Independent Bankers Association of Texas (*Registered, but did not testify:* Kathy Barber, NFIB; Jeff Burdett, Texas Cable Association; Celeste Embrey, Texas Bankers Association)

On — Wendy Reilly, The Technology Association of America; Matt Simpson, ACLU of Texas (*Registered, but did not testify:* Geoff Wurzel, TechNet)

BACKGROUND: Labor Code, subch. B governs unlawful employment practices.

DIGEST: CSHB 318 would add a new section to Labor Code, subch. B to prohibit an employer from requiring or requesting from an employee or job applicant a user name, password, or other means for accessing a personal account, including a personal e-mail account, a social networking website account, or a profile on an electronic communication device. "Electronic communication device" would be defined as a computer, telephone, personal digital assistant, or similar device to create, transmit, and receive information. An employer who violated the bill would be committing an unlawful employment practice.

The bill would allow an employer to access an employee's account if the employer had reasonable belief that the employee had violated federal or state law or an employment policy of the employer, including policies regarding:

- use of electronic devices for work-related communications;
- storing sensitive, private consumer information or proprietary information;
- employee cooperation in a workplace investigation; or
- the safety and security of employees or customers.

The bill would not prohibit employer policies on use of employer-provided electronic communication devices or the use of personal electronic devices during work, nor would it prohibit the monitoring of employee use of employer-provided electronic communication devices or employer-provided email accounts. The employer could lawfully obtain information in the public domain about the applicant or employee.

The bill would exempt state or local law enforcement agencies, as well as financial services employers. The latter would include depository institutions, mortgage bankers and residential mortgage loan companies, registered financial advisory firms, regulated loan companies, or insurance companies and agencies. CSHB 318 also would not apply to an employee of a financial services firm, securities exchange, registered securities association, or registered clearing agency using a personal social media account or electronic communications device to conduct business.

This bill would take immediate effect if finally passed by a two-thirds record vote of the membership of each house. Otherwise, it would take effect September 1, 2013.

SUPPORTERS SAY:

This bill would help safeguard employees' rights to privacy and free speech. Coercing an employee to hand over a password and user name to an online social media or email account is tantamount to eavesdropping and is an unfair exploitation of the power an employer holds over an employee. By passing this bill, the Legislature would give clear direction to employers and prevent the issue from being decided by the courts.

This bill would protect not only employees but employers. Employers who access applicants' or employees' social accounts may open themselves up to discrimination lawsuits should they discover information regarding protected status (such as sexual orientation, race, religion, disability, or political expression). Under the federal Health Insurance Portability and Accountability Act, an individual's health information is protected and confidential.

CSHB 318 is nuanced enough to allow employers a reasonable degree of latitude in complying with their other obligations while also protecting employees' rights. Employers could investigate violations of state and federal law or of workplace policies on the basis of a reasonable belief of wrongdoing. This would allow employers to consider evidence of harassment on an employee's personal account, for example, or of misleading advertisements of company goods or services sent in private by an employee in contravention of the Deceptive Trade Practices Act.

The bill would include a dispensation for the financial services industry, as those firms must comply with a different standard of communications under federal law. Employers must know whether employees have used accounts for illegal purposes in order to avoid liability under the Securities Exchange Act of 1934, the Truth in Lending Act, or other financial services-specific regulation.

CSHB 318 also would allow local and statewide law enforcement to access personal accounts of applicants or employees, an important exception that could protect public safety. Law enforcement agencies may need access to their employees' and applicants' accounts in order to determine whether they have affiliations with gangs or other groups or to discover other sensitive information. This dispensation for law enforcement agencies would enable a more thorough investigation into the character and background of potential hires and current employees. Employees who work in law enforcement offices should be held to a higher standard of scrutiny with respect to their personal conduct, as they hold positions of authority.

Employers still would have oversight over employee activity on employer-provided electronic devices and accounts, a fair exception.

OPPONENTS SAY:

This bill would hinder employers' ability to enforce workplace policies, including policies against harassment and bullying. Without active access to employees' social accounts, employers cannot monitor bad behavior. It can seriously hamper employers from preventing the leaking of trade secrets or proprietary information by employees, a key problem in industries reliant on strong protections for intellectual property, such as the technology industry. Employers could be held liable for their employees' online presence without being able to monitor or control it.

The bill's language would result in unintended consequences. Instead of prohibiting employers from asking for a username *and* a password, the bill would prohibit employers from asking for a user name *or* a password. On some social networking websites, a user's email address serves as a user name. The bill could have the effect of preventing employers from so much as asking for an employee's personal email address, important contact information that employers could legitimately need.

The bill would fail to define what is meant by a "personal account" of an employee or what constituted a "reasonable belief" by an employer before opening an investigation into an employee's personal account. The employer could be given broad latitude to search an employee's account when conducting an investigation, instead of limiting access to only the pertinent parts of an account. This addition would undercut seriously the prohibition against employer access and fail to define clearly the circumstances in which an employer can justify an investigation. "Reasonable belief" may in fact impose a positive duty on employers to monitor their employees' activity on personal accounts.

OTHER OPPONENTS SAY:

The bill is unnecessary. Employers know better than to go on an employee's personal account and expose themselves to knowledge that would render them liable.

The courts, not the legislature, should determine the boundary of an employee's right to privacy.

The bill would include too many exceptions to the prohibition against accessing an employee's personal account. Law enforcement and financial services companies would not have to comply with the general rule against requiring or coercing an applicant or employee's user name or password, and employers still could access the employee's personal account if conducting an investigation. The exemptions for law enforcement and financial services could result in the law being unevenly applied to different types of employers.

NOTES:

The committee substitute differs from the bill as filed by adding exemptions to the prohibition against employers accessing employees' personal accounts, including:

- exemptions to the bill for state and local law enforcement agencies,
- exemptions to the bill if the employer has reasonable belief the employee has violated state or federal law or workplace policies;
- exemptions for employers in the financial services industry and for any financial services employee who used the employer-provided account or device to conduct business.

CSHB 318 has a companion bill in the Senate, SB 118 by Hinojosa, which is identical to the bill as originally filed and was referred to the Business and Commerce Committee on January 29, 2013.