# Legislative Analysis

Mary Ann Cleary, Director
Phone: (517) 373-8080
http://www.house.mi.gov/hfa

**INTERNET PRIVACY PROTECTION ACT**

**House Bill 5523 as enacted**
**Public Act 478 of 2012**
**Sponsor: Rep. Aric Nesbitt**
**House Committee: Energy and Technology**
**Senate Committee: Energy and Technology**

**Complete to 1-15-13**

## A SUMMARY OF HOUSE BILL 5523 AS ENACTED

The bill would create a new act, to be known as the Internet Privacy Protection Act, which would, generally speaking, prohibit employers and educational institutions from requesting "access information" associated with "personal internet accounts" for prospective and/or current employees and students.

"*Access information*" would mean a user name, password, login information, or other security information that protects access to a social networking account. "*Social networking account*" would mean a personalized, privacy-protected website that allows an individual to (1) construct a public or semipublic profile within a bounded system established by an internet-based service and (2) create a list of other system users who are granted access to, and reciprocal communication privileges with, the individual's website.

Prohibited acts by an employer
Employers would be prohibited from (1) requesting an employee or applicant to disclose access information associated with a personal internet account; and (2) from discharging, disciplining, failing to hire, or otherwise discriminating against an employee or applicant for failing to disclose access information.

Prohibited acts by an educational institution
Educational institutions would be prohibited from (1) requesting a current or prospective student to disclose access information associated with that student's personal internet accounts; and (2) from discharging, disciplining, failing to admit, or otherwise discriminating against that student for failing to disclose personal internet account access information.

Permitted acts by an employer
The bill would not prohibit an employer from doing any of the following:

- Requesting or requiring an employee to disclose access information to the employer to gain access to or operate (1) an electronic communications device paid for in whole or part by the employer, or (2) an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for business purposes.

- Disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal internet account without prior authorization.

- Conducting an investigation or requiring an employee to cooperate in an investigation if (1) there is specific information about activity on the employee's personal account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related misconduct; or (2) the employer has specific information about an unauthorized transfer of the employer's proprietary or confidential information, or financial data to an employee's personal account.

- Restricting or prohibiting an employee's access to certain websites while using an electronic communication device paid for in whole or part by the employer or while using an employer's network or resources, in accordance with state and federal law.

- Monitoring, reviewing, or accessing electronic data stored on an electronic communications device paid for in whole or part by the employer, or traveling through or stored on an employer's network, in accordance with state or federal law.

The bill also would not prohibit or restrict an employer from (1) complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under federal law or by a self-regulatory organization, or (2) viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

Permitted acts by an educational institution

The bill would not prohibit an educational institution from requesting or requiring a student to disclose access information to the institution to gain access to or operate (1) an electronic communications device paid for in whole or part by the institution, or (2) an account or service provided by the institution that is either obtained by virtue of the student's admission to the institution or used by the student for educational purposes.

Educational institutions would also be allowed to view, access, or utilize information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

Employer and educational institution liability

The bill would not create a duty for an employer or educational institution to search or monitor activity on a personal internet account.

Neither an employer nor an educational institution would be liable under the bill for failing to request or require an employee, student, applicant, or prospective student to grant access to or disclose information that allows access to a personal internet account.

Penalties for violation

Anyone found in violation of the act would be guilty of a misdemeanor and subject to imprisonment up to 93 days and/or a maximum fine of $1,000.

Civil action

An individual who is the subject of a violation could bring a civil action and recover actual damages or $1,000, whichever is greater, and reasonable attorney fees and court costs. Except for good cause, not later than 60 days before filing a civil action, the individual would have to make a written demand of the alleged violator for the greater of the amount of the actual damages or $1,000. The written demand would have to include reasonable documentation of the violation and damages, and would have to be served in the manner provided by law for the service of process in civil actions or be sent by certified mail to the alleged violator's residence, principal office, or place of business.

Civil actions could be brought in the circuit court where the alleged violation occurred or in the county where the alleged violator resides or has a principal place of business.

It would be an affirmative defense to an action under this bill that the employer or educational institution acted to comply with the requirements of federal or state law.

**FISCAL IMPACT:**

To the extent that the bill's provisions result in additional misdemeanor convictions, the bill could result in increased costs to local correctional systems. These costs vary by jurisdiction. Any increased revenue from civil fines related to the bill would accrue local libraries, which are the constitutionally-designated recipients of this revenue. Local courts may face costs related to an increase in civil and criminal caseloads.

**BACKGROUND INFORMATION AND DISCUSSION:**

At issue is the expected privacy of current and/or prospective employees and students in relation to their personal internet accounts. According to testimony, the bill is designed to protect individuals against employers and educational institutions requiring an the disclosure of access information to a personal internet account (email, social networking, etc.) as a requirement for admission or hire. The practice gained national attention earlier this year when it was reported job applicants were being required to submit their login information for Facebook accounts as part of the application process. There have also been reports of universities requiring student-athletes to provide access to social media accounts. Employers believe access to these personal accounts is necessary to protect proprietary information and to limit liability on the party of the employer. However, others find the practice to be an invasion of privacy.

Concern was expressed during deliberations about the bill not exempting law enforcement agencies. Some believe that organizations charged with protecting public safety should have all available tools at their disposal during the screening and hiring process.

According to the National Conference of State Legislatures (NCSL), six states (California, Delaware, Illinois, Maryland, Michigan, and New Jersey) enacted legislation in 2012 prohibiting employers from requesting access information for personal internet accounts as a condition of employment. For more information, see:

http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx

Legislative Analyst: Jeff Stoutenburg
Fiscal Analyst: Bob Schneider
Erik Jonasson

■ This analysis was prepared by nonpartisan House staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.