

HOUSE BILL REPORT

HB 2278

As Reported by House Committee On:
State Government, Elections & Information Technology

Title: An act relating to enhancing personal information privacy protections in government entities.

Brief Description: Concerning personal information privacy protections in government entities.

Sponsors: Representatives Morris, Hudgins, Smith, Slatter, Tharinger, Macri, Young, Kloba and Appleton.

Brief History:

Committee Activity:

State Government, Elections & Information Technology: 1/16/18, 1/23/18 [DP].

Brief Summary of Bill

- Requires each state agency to designate a privacy officer to reduce the use and retention of personal information by the agency.
- Requires each privacy officer to report to the Office of Privacy and Data Protection by December 15, 2018.
- Prohibits government entities from selling personal identification numbers and personal financial and health information.

HOUSE COMMITTEE ON STATE GOVERNMENT, ELECTIONS & INFORMATION TECHNOLOGY

Majority Report: Do pass. Signed by 7 members: Representatives Hudgins, Chair; Dolan, Vice Chair; McDonald, Ranking Minority Member; Kraft, Assistant Ranking Minority Member; Appleton, Gregerson and Pellicciotti.

Minority Report: Do not pass. Signed by 1 member: Representative Irwin.

Minority Report: Without recommendation. Signed by 1 member: Representative Johnson.

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.

Staff: Sean Flynn (786-7124).

Background:

Privacy and Personal Information. Personal information and privacy interests are protected under various provisions of state law. Personal privacy is protected from unreasonable state intrusion under Article I, section 7 of the state Constitution. The Public Records Act (PRA), also protects a person's right to privacy under certain circumstances if disclosure would be highly offensive to the reasonable person, and is not of legitimate public concern. The PRA exempts personal information of public employees and officials maintained in public agency files from disclosure to the extent necessary to protect such person's right to privacy. Certain personal information related to investigative law enforcement records also is exempt from disclosure in order to protect a person's privacy.

The PRA also exempts certain personal information in public employee personnel records, including childcare enrollment, public employees and officials, tax assessments, personal financial information, driver's license records, vehicle license information associated with certain agencies conducting investigations, and 911 emergency systems contact information. Various other areas of state law protect privacy interests through confidentiality and other non-disclosure requirements.

Office of Privacy and Data Protection. In 2011 the Consolidated Technology Services (CTS) agency was created as part of a reorganization of state government information technology (IT) infrastructure functions and services. The CTS provides information services to public agencies, operates the State Data Center, and offers IT services, including data security and storage.

In 2016 the Office of Privacy and Data Protection (OPDP) was created within the CTS. The Chief Privacy Officer is appointed by the Chief Information Officer and serves as the Director of the OPDP. The OPDP is the central point of contact for state agencies on policy matters involving data privacy and protection, and provides annual privacy training for state agencies, coordinates agency data protection, conducts an annual review, and reviews major state agency projects involving personally identifiable information.

Summary of Bill:

Each state agency must designate a privacy officer to work with the OPDP to develop agency policy that reduces the use and retention of personal information. Each privacy officer must complete a training course through the OPDP at least every four years.

By December 15, 2018, each privacy officer must create a work plan to report to the OPDP. The work plan must take inventory of all personal information prepared and retained by the agency, including the type of information, the purpose for its collection, and the extent to which such information is protected from unauthorized disclosure.

The plan also must include a map of the physical and digital location of the personal information collected by the agency. Personal information includes a person's name, Social Security number, state driver's license or identification card, financial account numbers, credit or debit card numbers, and security codes. The inventory and map created for the work plan is exempt from public disclosure under the PRA to the extent it reveals the location of personal information.

A government entity is prohibited from selling personal identification numbers issued by a government entity. A government entity also is prohibited from selling personal financial and health information, including information that is identifiable to an individual and commonly used for financial or health care purposes, including account information and access codes or passwords, as well as information gathered for account security purposes or for account access, or information that relates to medical history or status.

Appropriation: None.

Fiscal Note: Available.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) Personal information can be collected and retained through various government operations, which creates a nexus between government function and privacy issues. The OPDP is the only resource for all state agencies regarding the management of private information. Agencies need in-house resources to advise policy on issues relating to privacy interests. Agencies need to evaluate their data collection methods and streamline their organizational process to only collect the type of information that is needed. Agencies already have public records officers, so in most cases this will not require new hires. The prohibition on selling personal information is good for protecting the privacy interests of private persons who interact with government services.

(Opposed) Certain driver's licensing information is shared by the Department of Licensing with insurance companies to verify driver records that is used to underwrite policies. This prohibition creates confusion with other statutes that allow for the sale of specific information, and should be clarified.

(Other) This would create confusion with other requirements that allow for the sale of certain specific information. This should not interfere with the public's ability to know the extent to which agencies are storing personal information. Some personal information is important to verify eligibility, such as birthdates, which are necessary to verify voter eligibility. This could prevent the practice of agencies selling information for important and legitimate reasons that benefit the public. The state has a substantial revenue stream from the sale of such information that would be lost if prohibited.

Persons Testifying: (In support) Representative Morris, prime sponsor; and Alex Alben, Office of Privacy and Data Protection.

(Opposed) Diana Carlen, RELX Inc.; and Cliff Webster, Consumer Data Industry and Thomson Reuters.

(Other) Rowland Thompson, Allied Daily Newspapers of Washington; and Mel Sorensen, Property Casualty Insurers Association of America and Allstate Insurance.

Persons Signed In To Testify But Not Testifying: None.