BILL ANALYSIS

C.S.H.B. 3278
By: Isett
State Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

A growing concern has been expressed across the nation regarding the security of private and personal information. With stories of identity theft, online stalking, and even violent crimes being attributed to the ease of obtaining otherwise personal information safeguards will be established to protect the information pertaining to law-abiding citizens. CSHB 3278 sets rules governing the use of social security numbers, driver's license numbers, and other sensitive information. The bill does not prohibit legitimate authorities or authorized persons from obtaining information and does not violate provisions of freedom of information acts. However, the bill does put in place rules to govern the dissemination of sensitive information such as bulk downloading, online records, and uses of social security numbers.

RULEMAKING AUTHORITY

It is the committee's opinion that rulemaking authority is expressly granted to the Department of Information Resources and to governmental entities as defined by Section 561.003(2), Government Code, in SECTION 4 of this bill.

ANALYSIS

Prohibits the capturing of biometric identifiers for commercial purposes. Prohibits storage of individual biometric identifiers; provides exceptions for law enforcement, federally-funded programs, credit unions, and programs designed to secure high-security areas. Prohibits certain uses of social security numbers and specifically permits other uses. Permits an individual to request that his/her social security number not be used and prohibits any denial of service, fee, or charge resulting from this request. Prohibits disclosure, sale, lease, or storage of a biometric identifier; provides exceptions for certain purposes.

Creates the Texas Privacy and Security Act which requires a commitment of governmental entities to strengthening privacy protections for personal information and to balance these strengthened privacy protections with the open records requirements and governmental accountability. Provides exceptions for access to information by law enforcement, private investigators, court officers, or persons accessing information under executive or legislative privilege.

Prohibits disclosure for certain personal information unless there is attorney general authorization determining that there is a compelling governmental interest in disclosure and that the information is especially relevant to an matter of intense public concern. Provides that a state or local governmental entity need not request an attorney general opinion before refusing to disclose social security numbers, bank account numbers, computer passwords, computer network locations or identities, or provide an individual's signature or a notary public's seal of office; requires the state or local governmental entity to inform the requestor why the information is being withheld and that the requestor is entitled to request the attorney general authorize the disclosure. Provides that Section 561.051 does not apply to information regarding a person deceased for seven or more years. Allows the attorney general to establish guidelines for state and local entities regarding privacy and security issues relating to request for public information and for sharing of information among governmental entities and the private sector.

Requires a state or local governmental entity to establish procedures for the collection of personal information. Requires state or local governmental entities to adopt and amend record

retentions schedules so that personal information is kept only for the necessary period of time. Requires state or local entities to develop, amend, and publicly post privacy policies.

Requires the Department of Information Resources (DIR) to adopt rules prescribing minimum privacy standards for internet sites and portals maintained by state of local governmental entities. Requires state or local governmental entities to adopt privacy policies consistent with the rules adopted by DIR relating to internet sites or portals and these policies are required to be included prominently in the general privacy policy as a separate element.

Requires the state auditor to establish auditing guidelines to ensure that state and local governmental entities do not collect unnecessary personal information and ensure those entities have information management systems that protect the privacy and security of information in their possession. Allows the state auditor to audit a state or local governmental entity for compliance with the guidelines the auditor has established.

Requires the open records steering committee established under Section 552.009 periodically to study and determine the implications for personal privacy of putting information on the internet, and to report those findings. Requires the Records Management Interagency Coordinating Council to provide guidance and policy direction to state and local governmental entities on electronic management of information.

Allows a governmental entity to impose conditions for remote access to governmental records, and deny access to a person who dies not comply with the conditions. Prohibits a governmental entity from transferring information in bulk unless the entity adopts rules to define what information may be posted online for download. Provides restrictions on a governmental entity's ability to contract with a third party for the gathering, storage, or creation in electronic format of the governmental entity's records. Allows an entity to impose a fee to conform with the applicable law regarding confidential information. Changes the penalty for fraudulent use or possession of identifying information to a third degree felony; this applies only to offenses committed on or after the effective date of the act, otherwise the former law in continued in effect.

EFFECTIVE DATE

Sections 1, 3, 4, 5, 6, 7, 8, 9 of the Act take effect September 1, 2005.
Section 2 of the Act takes effect January 1 2006.

COMPARISON OF ORIGINAL TO SUBSTITUTE

CSHB 3278 prohibits the capturing of biometric identifiers for commercial purposes. Prohibits storage of individual biometric identifiers; provides exceptions for law enforcement, federally-funded programs, credit unions, and programs designed to secure high-security areas.

CSHB 3278 provides that Chapter 142, Civil Practice and Remedies Code does not apply to a person who collects, uses, or releases a social security number if that person is required to do so by a federal or state law as it existed September 1, 2005.

CSHB 3278 provides that Chapter 142 controls to the extent of a conflict between that chapter and another state or federal law.

CSHB 3278 provides exceptions to the prohibition on storage of biometric identifiers in a database.

CSHB 3278 provides a definition for "sell" that states that is does not include the charge of a reasonable fee authorized or required by law for a copy of a document.

Creates the Texas Privacy and Security Act which requires a commitment of governmental entities to strengthening privacy protections for personal information and to balance these strengthened privacy protections with the open records requirements and governmental accountability. CSHB 3278 provides exceptions for access to information by law enforcement, private investigators, court officers, or persons accessing information under executive or

legislative privilege. States that except where otherwise provided in the bill or expressly by other law, the provisions of this bill control. CSHB 3278 provides that this bill does not affect the ability of state or local governmental entities to undertake lawful investigations.

CSHB 3278 provides that a state or local entity is not required to request an attorney general opinion before refusing to provide and individual's signature or the seal of office of a notary public.

CSHB 3278 provides that Section 561.051 does not apply to information regarding a person deceased for seven or more years.

CSHB 3278 requires that the rules adopted by DIR provide that personal information stored online must be unavailable to unauthorized persons and that the rule require that the internet site or portal have security measures to prevent an unauthorized person from downloading personal information in bulk.

CSHB 3278 adds subchapter D providing restrictions on remote access, allowing governmental entities to impose conditions on or refuse remote access to governmental records.

CSHB 3278 provides restrictions on a governmental entity's ability to contract with a third party for the gathering, storage, or creation in electronic format of the governmental entity's records. Allows an entity to impose a fee to conform with the applicable law regarding confidential information.