TLTA's Responses to the Texas Privacy Protection Advisory Council Survey

Q1: Are there laws in Texas, other states, or relevant jurisdictions which govern the private sector in the privacy and protection of information which should be considered by the Texas Privacy Protection Advisory Council?

TLTA's Answer to Q1:
Yes. There are a number of sector-specific federal privacy laws that should be considered by the Council. Any new privacy law enacted by a state which conflicts with the federal laws creates great challenges for industry. We encourage state legislators to include an exemption within any state privacy law for businesses already regulated by a federal privacy law. An alternative is to recognize in the state law that the business's compliance with the federal privacy is deemed compliance with the state law.

There are sector-specific privacy laws at the state level as well. For example, in the insurance and financial services space, the federal Gramm-Leach-Bliley Act (GLBA) sets privacy requirements for title insurance companies. However, states have historically regulated insurance activities. To harmonize GLBA with the historical state regulation of insurance, GLBA mandated that insurance activities would be "functionally regulated" by the States (GLBA § 301, 15 U.S.C. §6711).

To this end, while insurance companies, agents and insurance brokers are "financial institutions" under GLBA and thus are subject to GLBA's Privacy and Safeguards Rules, the GLBA privacy and security requirements are enforced under state insurance law by state insurance regulators for "any person engaged in providing insurance." (GLBA § 505(a) (6), 15 U.S.C. § 6805(a) (6)).

After GLBA's enactment, and in response to the enforcement provisions under GLBA, both the National Association of Insurance Commissioners ("NAIC") and the National Conference of Insurance Legislatures ("NCOIL") issued proposed model privacy acts that satisfy the GLBA's privacy requirements. Texas adopted the NAIC model privacy law. Texas's Insurance Consumer Financial Information Privacy law is codified at 28 TEX. ADMIN. CODE §§ 22.1 to 22.27 and §§ 22.51 to 22.67.

The Texas insurance privacy law applies to all insurance companies and producers that are selling insurance in Texas or covering insurance risks in the state. Without the reference to the state insurance privacy law, and an exemption for those in compliance with that law, in any Texas comprehensive privacy law meant for states' adoption, state lawmakers would be creating holes in the enforcement framework for the insurance industry that would be of significant concern for the Texas Department of Insurance and its regulated entities.

Q2: Are there laws in Texas, other states, or relevant jurisdictions which govern the public sector in the privacy and protection of information which should be considered by the Texas Privacy Protection Advisory Council?

TLTA's Answer to Q2:
Our experience with the levels of state government and the political subdivisions that our industry interfaces with is that they do an excellent job protecting necessary private information (ie. Texas

Department of Insurance, County Clerks and District Clerks). We urge extreme caution when addressing information traditionally considered public information. Many industries, services, and necessary commercial functions depend on access to this traditional information to serve consumers and help insure a healthy and strong real estate economy.

Q3: What key components of privacy and protection of information that is linked to a specific individual, technological device, or household should be considered by the Texas Privacy Protection Advisory Council?

TLTA's Answer to Q3:
The American Land Title Association (ALTA) has developed principles regarding data privacy to help guide state law makers around the nation. Below are several key principles for your consideration.

Gramm-Leach-Bliley Act (GLBA) Exemption
Any comprehensive data privacy legislation should include a full entity exemption for entities subject to the GLBA. Since 1999, this federal law has strictly limited financial institutions' use and sharing of customers' personal information. Additionally, financial institutions are required to assure the security of this information and provide comprehensive disclosures to consumers.

Publicly Available Information Exemption
Personal information that is lawfully made available from federal, state, or local government records is already, by definition, public information and should be exempted from any data privacy legislation. It serves no public policy purpose to have a subsequent procurer of public information treat it as private information.

Recognize the Necessities of Transaction-Based Data Transfers
Data privacy laws should recognize and protect businesses' legitimate bases for processing personal information. Portability or deletion rights should not impede a business or service provider's ability to process a consumer's personal information to, among other things:

- Complete a transaction or provide a good or service.
- Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- Enable internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
- Comply with a legal or regulatory obligation.
- Otherwise use the consumer's personal information in a lawful manner that is compatible with the context in which the consumer provided the information.

Small Business and Risk-Based Considerations
In crafting data privacy law, consideration should be given to the impact on small business, with respect to the cost of compliance relative to the risk of consumer harm. This can be accomplished by establishing a threshold based on revenue and/or volume of consumer data handled that triggers more rigorous data privacy standards for businesses. For the sake of consistency, standards used for the applicability of data privacy requirements in other states should be considered.

Right to Cure

A right to cure should be included in standards for enforcement of data privacy or security laws. This gives companies the ability to address and fix technical violations before an issue causes consumer harm.

Business-to-Business Exemption
Personal information collected within the context of business-to-business relationships should be exempt from data privacy regulations.

Employee Exemption
Except for disclosures and notifications related to data security breaches, job applicant and employee data used for a business purpose should be excluded from data privacy law requirements.