ALTA's Principles for Data Privacy Laws

The American Land Title Association (ALTA), which represents the real estate settlement services, abstract and title insurance industry, has been a long-time advocate for efforts to protect the personal information of consumers. Since 2013, industry standards encompassed in ALTA's Best Practices have included requirements for a written privacy and information security program to protect non-public personal information.

The conversation occurring nationally on data privacy is an important one. To help better engage in these discussions, ALTA has developed principles for data privacy laws to guide these conversations so that our member companies can continue to offer consumers an efficient home buying or selling experience, while at the same time protecting private information uniformly and consistently.

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.

National Standards

Today, business occurs across state lines as frequently as within them. A patchwork of state privacy laws creates inconsistent protections for consumers and confusion for both consumers and businesses seeking to understand these statutes and compliance obligations. A single federal standard eliminates both the disparity and confusion.

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.

Data Breach Notifications
Given the prevalence of interstate commerce, data breach notification legislation should be uniform throughout the country, providing clear notification requirements. Notifications to both regulators and consumers should be required within a reasonable time frame. Notification to consumers should only be required when there is a reasonable likelihood of materially harming consumers.

Safe Harbor
Businesses that maintain and comply with a cybersecurity program that reasonably conforms to an industry-recognized cybersecurity framework should be provided a legal safe harbor for data breach-related claims. A safe harbor encourages investment in the resources to protect the security of information, while creating legal certainty for businesses.

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.