CARLTON FIELDS

The Basics of U.S. Privacy Rights

The United States does not have a single, federal law establishing a business' privacy obligations regarding the collection, use, and security of personal information. The current system is an overlap between federal and state laws and regulations, including sector-specific laws, common law principles, and contract principles. Below, we summarize some pieces of this legal landscape, with a particular focus on laws and regulations that may apply to providers in a real property transaction.

Federal Laws and Regulation

The Gramm-Leach-Bliley Act (GLBA)

The GLBA applies to financial institutions and impacts the collection, use, safekeeping, and disclosure of nonpublic personal information (NPI). Financial institutions include banks, securities firms, insurance companies, mortgage lenders or brokers, and other businesses that provide financial services and products. The GLBA requires that financial institutions (1) notify customers about their information sharing practices; (2) provide customers with a right to opt-out if they do not want their information shared with certain unaffiliated third parties, as detailed in the GLBA Financial Privacy Rule; and (3) implement a written information security program (WISP), including specific safeguards to protect NPI from unauthorized disclosure, as detailed in the GLBA Safeguards Rule.

The Federal Trade Commission Act (FTC)

The FTC Act is not specifically a privacy and data security law; its broad focus is on unfair or deceptive commercial practices. The FTC has been active, though, in using the FTC Act and regulations under it, to police what it sees as unfair or deceptive practices in the collection, use, processing, protection, and disclosure of personal information. Two areas of enforcement risk are (1) failing to comply with statements in posted privacy policies, or making material changes to those policies without adequate notice, and (2) failing to provide reasonable and appropriate security measures for sensitive consumer information. The FTC also issues privacy and data security guidelines that are not legally binding but could be considered best practices, even for businesses that have a different primary regulator.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies to most health care providers, health plans, and their service providers, which can include businesses that have their own health plans. The HIPAA Privacy Rule applies to the collection, use, and disclosure of protected health information. The HIPAA Security Rule provides standards for safeguarding that information. An entity that acts on behalf of an entity covered by HIPAA is known as a business associate, and those business associates typically have contractual obligations to safeguard this information derivative of their relationship with the covered entity.

Fair Credit Reporting Act (FCRA) as amended under the Fair and Accurate Credit Transactions Act (FACTA)

FCRA/FACTA regulates consumer credit and other information, and limits how consumer reports (which include creditworthiness or credit history) and credit card account numbers can be used and disclosed. It applies to consumer reporting agencies, businesses that use consumer reports (such as lenders and employers), and others, such as credit card companies. Under FACTA, the FTC has promulgated the Red Flags Rule, which requires financial institutions and creditors to implement and maintain written identity theft prevention programs.

CARLTON FIELDS

The Basics of U.S. Privacy Rights

State Laws and Regulation

A number of states have adopted laws and regulations related to consumer privacy. Below, we note and discuss briefly a few of the more prominent state laws.

California

California was the first U.S. state to enact a comprehensive consumer privacy law, The California Consumer Privacy Act, in 2018. It was amended in 2020 by the California Privacy Rights Act. This law provides California residents with certain rights with respect to their personal information, including the right to data portability, to delete personal information, and to opt-out of the sale or sharing of personal information. The law has a data-level exemption for GLBA personal information.

Virginia, Colorado, Connecticut, and Utah

Virginia, Colorado, Connecticut, and Utah have laws that provide rights similar to those provided in California, including a consumer's right to access personal information, a right to delete, and a right to opt-out of sale. In contrast to California, these states each have entity-level GLBA exemptions. Other states either do not have comprehensive privacy laws or have privacy laws that are limited to data brokers or are sector-specific.

New York

New York's Department of Financial Services has adopted a comprehensive rule on cybersecurity requirements for Financial Services Companies. This rule applies to insurance companies, banks, and other financial services institutions that are licensed, or based, in New York. While the rule largely focuses on security governance, it does require a covered business to conduct a risk assessment and maintain a cybersecurity policy that addresses customer data privacy and data governance and classification.

Massachusetts

While Massachusetts does not have a comprehensive privacy law, it does require that any business that owns or licenses personal information about a resident of the state maintain a comprehensive WISP.

Private Contract

PCI DSS

A business that processes credit card payments must satisfy a number of specific privacy and security requirements. These apply through a series of contractual relationships among the business, the business's merchant bank, and the credit card brands. These agreements incorporate standards from the PCI Security Standards Council, known as the Payment Card Industry Security Standard (PCI DSS).

Contracts with Consumers

A business may promise certain privacy standards to its customers through contract, such as terms and conditions, terms of use, end-user licensing agreements, or a similar arrangement. Additionally, liability might arise through common law principles for representations made in a privacy policy or privacy notice if those representations are inaccurate.

Contracts with Other Businesses

Many businesses have substantial commitments to privacy and cybersecurity that are part of business-to-business contracts, particularly if the transaction involves the transfer, collection, or use of personal information. Federal or state law may impose specific contractual language for these types of contracts, which are often known as service provider agreements or data processing agreements or addenda.

Contacts

John E. Clabby
jclabby@carltonfields.com
www.carltonfields.com/jclabby
813.229.4229

Patricia M. Carreiro
pcarreiro@carltonfields.com
www.carltonfields.com/pcarreiro
305.539.7314

Joseph W. Swanson
jswanson@carltonfields.com
www.carltonfields.com/jswanson
813.229.4335

Eden Marcu
emarcu@carltonfields.com
www.carltonfields.com/emarcu
813.229.4148