Data privacy basics – US compliance overview

In contrast to most European privacy regimes, US privacy law is a complex patchwork of privacy laws and regulations addressing specific industries, communications media, or marketing methods, supplemented by a backdrop of federal and state prohibitions against unfair or deceptive business practices, and state laws that specifically address privacy and security of personal information.

What federal laws govern data privacy?

The United States has not adopted a comprehensive federal privacy and data security law like the European Union. Instead, the United States has implemented a sectoral approach to data privacy, promulgating regulations in areas that it deems to be of specific concern, including financial data, credit data, background checks, health information, telecommunications companies, video rental records (which may include certain video streaming services), drivers' license information and history, children's information, and marketing.

Is information about children subject to privacy regulation?

The Children's Online Privacy Protection Act and its promulgating rules (collectively, "COPPA") strictly regulate the collection of personal information online from children under 13 years old by operators of website, mobile apps and other online services. If a company collects any personal information online (including through mobile apps) directly from children under 13, it will be required to comply with COPPA.[1] Among other things, COPPA requires that an operator of site or mobile app that collects information from children (i) distribute a "Direct Notice" of privacy practices to parents, (ii) publish a COPPA-compliant privacy policy, and (iii) obtain verifiable parental consent from parents *prior* to collecting personal information from children under 13.[2]

On the other hand, COPPA does not apply to information collected about children, from adults. So, for example, if a coach uploads a team roster and other information to a website, that would not be subject to COPPA; however, if a child were able to then access the website and submit additional information to it, the information submitted by the child would be subject to COPPA.

What laws govern financial privacy?

The Gramm-leach-Bliley Act (GLBA) applies to "financial institutions'" collection, use, disclosure and safeguarding of "nonpublic Personal Information." The definition of financial institution is broad, and may apply to companies (*ie*, nonbanks) offering consumers finance plans or lines of credit for use in personal, family or household purposes. Nonpublic Personal Information is any Personal Information provided to a financial institution by a consumer. Many financial institutions subject to GLBA must provide their consumer customers with an annual privacy notice. Further, all financial institutions subject to GLBA are limited in how they may use and share Nonpublic Personal Information, must provide adequate safeguards for nonpublic Personal Information, and have certain obligations to notify regulators and customers in the event of a data security breach.

Both federal and state laws require protections for and strictly limit the use of consumer reports (*ie*, credit reports and

background checks). Consumer reports are any information provided, in any medium, by a consumer reporting agency that will be used for decisions related to consumer credit, employment, or insurance purposes. Persons may only obtain a consumer report from a consumer reporting agency if the person has a permissible use for that data. Persons obtaining consumer reports must provide adequate safeguards and properly dispose of the consumer report information. If a person takes an adverse action against a consumer because of information contained in a consumer report (*ie*, denies credit or employment), the person must provide the consumer with a written notice. Federal law provides consumers with a private right of action for the misuse of their consumer reports.

Federal regulations also apply to business reporting data to consumer reporting agencies (*ie*, defaults or delinquencies), requiring the data furnisher to ensure the reported information is accurate and to investigate consumer disputes.

Are educational records and student privacy regulated?

The federal Family Educational Rights and Privacy Act (FERPA) protects students' educational records at educational institutions who accept federal funding. Educational records are broadly defined, with a limited exception for directory information, such as names, addresses, and phone numbers. FERPA prohibits the disclosure of educational records without the prior approval of the student or parent. Educational institutions who share educational records, with, for example, service providers, are required to pass on their FERPA compliance obligations via contract. While FERPA violations are technically enforced against the educational institution, violations could lead to sanctions on a service provider, such as prohibiting them from receiving educational records or damages for breach of contract with the educational institution.

A number of states recently enacted laws limiting how online services could collect or use student information that is collected when providing an application or service for school purposes. Some of these laws apply only to educational institutions, while some also apply to service providers of educational institutions.

Is electronic marketing regulated?

US federal law also specifically governs marketing by email (CAN-SPAM Act), telephone and text messages (Telephone Consumer Protection Act, Do-Not-Call Registry and related FTC and FCC Rules) and facsimile. For example, the CAN-SPAM Act requires companies that send commercial emails to any person or entity (1) only send such emails to recipients who have not opted out; (2) provide recipients a cost-free and easy way to opt out of future emails, which the sender must honor within ten (10) business days; and (3) include specific information in all commercial emails.

Sending text messages to mobile phones is another highly regulated activity, under federal law, which requires prior, specific and express consent from individuals to send any SMS messages (marketing or otherwise). The sending of SMS messages is currently a very high class-action risk area. In order to mitigate risks in this area, it is vital to work with legal counsel to compose appropriate consent language and processes. Federal telemarketing rules also impose a number of specific restrictions and obligations on any company that engages in telemarketing to consumers. Telemarketing is also subject to specific regulations and requirements in states, which may (depending upon the state) impose additional or more stringent rules than the federal ones.

Outside of the sector-specific laws, to protect consumer privacy, the Federal Trade Commission ("FTC") relies on its authority under Section 5 of the FTC Act, which prohibits entities from engaging in unfair and deceptive trade practices. In evaluating whether entities are engaging in "unfair and deceptive trade practices," the FTC examines whether the entity has provided appropriate notice to consumers about its privacy or other practices that are in question. The FTC has found that a

failure to provide appropriate notification about the information collected and/or the failure to abide by representations made in privacy policies (including those about information security) are unfair and deceptive trade practices.

Are there any state data privacy laws?

The US has fifty states, each with its own consumer privacy and protection framework. Myriad state laws address privacy-related issues, such as requirements for data security, compliance with PCI-DSS, storage of data, disposal of data, privacy policies, appropriate use of social security numbers, data breach notification, employee privacy laws, telemarketing, and privacy of education information. States also have consumer protection laws that seeks to protect consumers against unfair and deceptive trade practices, and state attorneys general typically enforce these laws against businesses (though, in some states a private right of action is available against companies that violate state consumer protection laws).

State privacy laws typically track the location of the data subject. Thus, even if a company does not have an office and/or employees in a particular state, it will still likely be subject to the privacy and data security laws in the state if it has a customer in that state. Since most e-commerce companies will likely serve customers throughout the United States, we recommend that clients be familiar with the various state requirements, including laws pertaining to third-party service providers, marketing, data breaches, written information security plans, and data destruction. California law, in particular, has a number of different privacy laws that apply to companies that collect information about or sell products and services to residents of California.

A number of states have passed laws that restrict employers from requesting or requiring employees and job applicants provide access to their personal social media (in some cases including email) accounts, subject to some specific exemptions.

A number of states have passed laws restricting collection and transmission of Social Security numbers (SSNs). Most prohibit a company from: (i) publically displaying SSN, (ii) printing SSN on mailed forms (with certain exceptions, such as tax forms) or embedding it within access or other ID cards, (iii) requiring an individual to submit an SSN over an unencrypted connection, (iv) requiring an individual to use SSN to access a website or online service, unless a personal identification or other password is also required, and (v) selling SSNs.

[1] COPPA broadly defines personal information to include name, address (including street name + city), email address, phone number, online contact information, and geolocation information, as well as photos, videos, voice recordings, and IP address, device identifiers and any other unique identifiers that can be used to track children over time and across sites or apps.

[2] COPPA sets forth some very specific mechanisms (*eg*, printing and mailing to emailing a signed consent form, calling a toll free number to provide consent, processing a credit card transaction) for obtaining verifiable parental consent. While the mechanisms set forth in the rule are not exclusive, simply getting a parent to tick an "I Agree" box online will not be sufficient.