DATA PROTECTION LAWS OF THE WORLD

United States vs Laos

DLA PIPER

UNITED STATES

Last modified 29 January 2023

LAW

United States privacy law is a complex patchwork of national, state and local privacy laws and regulations. There is no comprehensive national privacy law in the United States. However, the US does have a number of largely sector-specific privacy and data security laws at the federal level, as well as many more privacy laws at the state (and local) level. In recent years, beginning with California, states have begun to introduce their own comprehensive privacy laws, and other states are expected to follow and enact their own comprehensive state privacy laws. Although a bipartisan draft bill (the ‘American Data Privacy and Protection Act’) was introduced in 2022, several senators were in opposition of the bill, and comprehensive privacy law on the federal level is not expected to pass any time soon.

Federal and State Privacy Laws and Regulations

Federal laws and regulations include those that apply to financial institutions, telecommunications companies, credit reporting agencies and healthcare providers, as well as driving records, children’s privacy, telemarketing, email marketing and communications privacy laws.

There are also a number of state privacy and data security laws that overlap with federal law—some of these state laws are preempted in part by federal laws, but others are not. US states have also passed privacy and data security laws and regulations that apply across sectors and go beyond federal law—such as data security laws, secure destruction, Social Security number privacy, online privacy, biometric information privacy, and data breach notification laws. Generally, each state’s laws apply to personal information about residents of that state or activities that occur within that state. Thus, many businesses operating in the United

LAOS

Last modified 24 January 2024

LAW

In Laos, the comprehensive regulatory framework on data privacy focuses on data in its digital form – electronic data – and none other.

From 2012, Laos has introduced this framework by circulating relevant information only. This trend has accelerated since 2015 with the publication of the Law on Cyber Crime. Issues pertaining specifically to the protection of electronic data are regulated by the Law on Electronic Data Protection and the subsequent Instructions on the Implementation of the Law on Electronic Data Protection, as follows:

- Law on Electronic Transactions (2012)
- Law on Cyber Crime (2015)
- Decision on the Penalties of the Law on Cyber Crime (2017)
- Law on Electronic Data Protection (2017)
- Penal Code (2017)
- Instructions on the Implementation of the Law on Cyber Crime (2018)
- Instructions on the Implementation of the Law on Electronic Data Protection (2018)

In addition, for both professionals or non-professionals, the authorities have provided a series of guidelines of best practices for the use of software and hardware, social media platforms, and better protection of electronic data.

The two main pieces of regulation relating to data privacy are the Law on Electronic Data Protection and the Instructions on the Implementation of the Law on Electronic Data Protection.

States must comply not only with applicable federal law, but also with numerous state privacy and security laws and regulations.

For example, California alone has more than 25 state privacy and data security laws, including the California Consumer Privacy Act (CCPA) and its regulations as recently amended by the California Privacy Rights Act (CPRA), collectively referred to as the CCPA. The CCPA, as amended, introduced additional definitions and individual rights, and imposed additional requirements and restrictions on the collection, use and disclosure of personal information. The CCPA is also unique among state comprehensive privacy laws in that, as of January 1, 2023, it applies to HR and B2B personal information. Enforcement of the CPRA amendments to the CCPA commenced on July 1, 2023 for violations of the new provisions that occur on or after that date.

Notably, updated CCPA regulations based on the CPRA amendments were finalized on March 29, 2023, with enforcement by the California Attorney General and the newly established California Privacy Protection Agency (‘CPPA’ or ’Agency’) expected to begin on July 1, 2023. However, following a suit filed by the California Chamber of Commerce, the Sacramento district court ruled that the Agency was required to give businesses 12-months between finalizing a CCPA regulation and commencing enforcement, effectively delaying enforcement of the amended regulations to March 29, 2024. This delay does not affect the Agency or the California Attorney General’s ability to enforce the version of the CCPA amended by the CPRA (effective July 1, 2023) or the existing (i.e., pre-2023-amendment) CCPA regulations (effective August 14, 2020).

In late 2022, the California legislature also passed the California Age-Appropriate Design Code, which was slated to take effect July 1, 2024 and would apply to companies that meet the definition of “ business” under the CCPA and that provide online services that are likely to be accessed by individuals under 18 years of age. However, on September 18, 2023, a California District Court issued an injunction blocking the law from coming into effect on First Amendment grounds. Following an appeal to the Ninth Circuit by the California Attorney General's office, the fate of the law is currently uncertain. More information on the California Age-Appropriate Design Code can is available at https://www.dlapiper.com/en-us/insights/publications/2023/05/californias-age-appropriate-design-code-act

Beyond California, Colorado's Attorney General finalized the Colorado Privacy Act (CPA) Rules on March 15, 2023, which add significantly to the CPA’s obligations on businesses. Both the CPA and the CPA Rules went into effect July 1, 2023. Connecticut, Utah, and Virginia’s privacy laws also took effect in 2023.

While not identical, the Colorado, Connecticut, Utah, and Virginia state privacy laws are substantially similar to each other in most key aspects. Further, unlike the CCPA, all are also generally inapplicable to personal information collected about, and processed in the context of, employee and business relationships. On the other hand, while the CCPA has some practical similarities with these state laws, it adopts more granular definitions, requirements, and restrictions that vary considerably from these laws, and, notably, applies to personal information collected from California residents in employment and B2B contexts.

2023 brought a significant development in the health data space, with Washington passing the My Health My Data Act (MHMD). The law ostensibly applies only to consumer health data, but its exceptionally broad definitions and scope combined with its private right of action may mean its enforcement touches on data many companies may not typically consider “ health” data. More information on the MHMD Act is available at https://www.dlapiper.com/en/insights/publications/2023/04/washington-state-passes-my-health-my-data-act

Finally, the pace of state privacy legislation accelerated in 2023 overall, with the following states passing their own comprehensive privacy laws or variations thereof:

- Florida (effective July 1, 2024)
- Oregon (effective July 1, 2024)
- Texas (effective July 1, 2024)
- Montana (effective Oct. 1, 2024)
- Delaware (effective Jan. 1, 2025)
- Iowa (effective Jan. 1, 2025)
- Tennessee (effective Jan. 1, 2025)
- New Jersey (effective Jan. 15, 2025)
- Indiana (effective Jan. 1, 2026)

More information on the US state privacy laws is available at https://privacymatters.dlapiper.com/state-privacy-laws/

Enforcement of Unfair and Deceptive Trade Practices

In the United States, consumer protection laws, which prohibit unfair and deceptive business practices, provide another avenue for enforcement against businesses for their privacy and security practices.

At the federal level, the US Federal Trade Commission (FTC) uses its authority to protect consumers against unfair or deceptive trade practices, to take enforcement actions against businesses for materially unfair privacy and data security practices. The FTC uses this authority to, among other things, take enforcement actions and investigate companies for:

- Failing to implement reasonable data security measures
- Making materially inaccurate or misleading privacy and security statements, including in privacy policies
- Failing to abide by applicable industry self-regulatory principles
- Transferring or attempting to transfer personal information to an acquiring entity in a bankruptcy or M&A transaction, in a manner not expressly disclosed on the applicable consumer privacy policy
- Violating consumer privacy rights by collecting, using, sharing or failing to adequately protect consumer information, in violation of standards established in their prior enforcement precedents

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. State attorneys general also sometimes work together on enforcement actions against companies for actions that broadly affect the consumers of multiple states (such as data breaches).

Privacy class actions also continue to be a key risk area in the United States, including in the context of biometric privacy (under the Illinois Biometric Privacy Act), text messaging (under the federal Telephone Consumer Privacy Act) and call recording, wiretapping and related claims under the California Invasion of Privacy Act and other state laws. Online monitoring and targeting activities—including via cookies, pixels, chat bots, and so-called “session replay” tools— are an area of particular focus in the United States from a regulator and enforcement perspective and are also a developing litigation risk area.

DEFINITIONS

Definition of personal data

Varies widely by law and regulation. The definition of personal information varies under US law. Some laws—such as data breach and security laws— apply more narrowly, to sensitive personal information, such as government identifiers, financial account information, password, biometrics, health insurance or medical information, and other information that can lead to identity fraud and theft or financial harm. On the other hand, under a number of state and federal laws, personal information broadly includes any information that identifies or is linked or reasonably linkable to an individual.

California

Under the CCPA, personal information includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The definition specifically includes name, alias, contact information, government IDs, biometrics, genetic data, location data, account numbers, education history, purchase history, online and device IDs, and search and browsing history and other online activities, if such information is linked or linkable with a particular consumer or household. Excluded from the definition are deidentified information and information lawfully made publicly available through various means, such as through government records or by the consumer.

Under the law, 'consumer' is broadly defined as any resident of California.

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia

Under the other thirteen comprehensive state privacy laws, personal data includes information that is linked or reasonably linkable to an identified or identifiable individual, who is a resident of the particular state acting an individual or household capacity. Deidentified data, personal data made publicly available, and personal data about individuals acting in an employment or B2B context are generally not in scope.

Definition of sensitive personal data

Varies widely by sector and by type of statute.

DEFINITIONS

Definition of Personal Data

Article 3, Section 12 of the Law on Electronic Data Protection defines “personal data” to mean electronic data of an individual, legal entity, or organization.

Definition of Sensitive Personal Data

The Law on Electronic Data Protection aims to protect any type of electronic data. The law categorizes electronic data roughly into three types: (i) general data, (ii) sensitive data (a literal translation would be “ specific data”), and (iii) prohibited data. Depending on its nature, personal data may fall under one these three categories. Accordingly, there is no “ sensitive personal data” so to speak. Given this, personal data may fall under the category of sensitive data.

Sensitive data is information “that an individual, legal entity, or organization cannot access, use, or disclose if [they] have not received consent from the Information Owner, or the relevant organization” (Article 10).

A list of examples of sensitive data is provided in the Instructions on the Implementation of the Law on Electronic Data (2018), which includes “ information on customers, financial information, CV, history of medical treatment, race, religion, project plan, budget plan, official servant secret, etc.” (Section 3). The list is not exhaustive, and there is no official guidance to anticipate what other data may be considered sensitive data apart from these examples.

Generally, includes personal health data, financial data, credit worthiness data, student data, biometric data, personal information collected online from children under 13, and information that can be used to carry out identity theft or fraud are considered sensitive, and subject to additional restrictions and regulations.

For example, state breach notification laws and data security laws generally apply to more sensitive categories of information, such as Social security numbers and other government identifiers, credit card and financial account numbers, passwords and user credentials, health or medical information, insurance ID, digital signatures, and /or biometrics.

California

The CCPA defines *sensitive personal information* as personal information that reveals about a consumer one or more of the following types of information, including:

- Social Security, driver’s license, state identification card or passport number
- account log-in, financial account, debit card or credit card number in combination with any required security or access code, password or credentials allowing access to an account
- precise geolocation
- racial or origin, citizenship or immigration status, religious or philosophical beliefs, or union membership
- contents of a consumer’s mail, email, and text messages unless the business is the intended recipient of the communication
- genetic data
- biometric information
- health information
- information about sex life or sexual orientation

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia

Under the other thirteen comprehensive state privacy laws, the definition of *sensitive data* is a sub-cateogry of peronsal data and largely the same with various states adding or subtracting certain data elements from the above list.

Washington

Washington’s MHMD Act introduced a very broad definition of *consumer health data*, which includes: “personal information that is linked or reasonably

linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status."

For the purposes of this definition, physical or mental health status includes, but is not limited to:

- Individual health conditions, treatment, diseases, or diagnosis
- Social, psychological, behavioral, and medical interventions
- Health-related surgeries or procedures
- Use or purchase of prescribed medication
- Bodily functions, vital signs, symptoms, or measurements of the information described in subsection (8)(b)
- Diagnoses or diagnostic testing, treatment, or medication
- Gender-affirming care information
- Reproductive or sexual health information
- Biometric data
- Genetic data
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies
- Data that identifies a consumer seeking health care services
- Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in (b)(i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)

This definition could arguably include any category of personal data (e.g., the inclusion of inference data makes it difficult to exclude any data whatsoever in the health, wellness, and fitness space). In addition, “health care services” includes any service provided to a person to assess, measure, improve, or learn about a person's health.

NATIONAL DATA PROTECTION AUTHORITY

There is no single national authority.

With some exceptions (such as for banks, credit unions and insurance companies), the FTC has jurisdiction over most commercial entities and has authority to issue and

NATIONAL DATA PROTECTION AUTHORITY

The Law on Electronic Data Protection (2017) originally delegated the Ministry of Post and Telecommunications (MPT) to handle matters related to the protection of electronic data. The MPT has now been renamed Ministry

enforce federal privacy regulations (including telemarketing, email marketing, and children's privacy) and to take enforcement action to protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices.

Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states.

California

The California Attorney General and the California Privacy Protection Agency (the Agency) share authority to enforce the CCPA.

California consumers also have a private right of action under the CCPA for certain data breaches, and the CCPA provides for statutory damages.

Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, New Jersey, Oregon, Tennessee, Texas, Utah, Virginia

State Attorneys General in all the other thirteen states have authority to enforce their state comprehensive privacy laws. Additionally, in some states such as Colorado, district attorneys can enforce the law.

None of these states currently provide for a private right of action.

Washington

The Washington Attorney General has the authority to enforce the MHMD Act.

Washington residents also have a private right of action under the Act, but unlike the CCPA the MHMD Act does not provide for statutory damages, meaning plaintiffs must prove actual damages to succeed.

Sector-Specific Enforcement

In addition, a wide range of sector-specific regulators, particularly those in the healthcare, financial services, telecommunications and insurance sectors, have authority to issue and enforce privacy and security regulations, with respect to entities under their jurisdiction.

REGISTRATION

of Technology and Communication (MTC) and is the main administration in charge of issues pertaining to electronic data privacy across the country. The MTC is assisted by its departments located in each of the 17 provinces that compose Laos.

In its tasks to analyze and respond to digital issues and threats, the MPT was originally assisted by the Lao Computer Emergency Response Team (LaoCERT), which was established in 2012. LaoCERT is now a Division under direct supervision of the Department of Cyber Security in the MTC and is the agency on the front lines that receives reporting of security breaches from individuals or legal entities operating in Laos and / or complaints of offenses committed online.

REGISTRATION

There is no requirement to register databases or personal information processing activities. However, four states currently impose certain registration requirements on data brokers:

California

The CCPA (as amended in 2019) requires (subject to some exceptions) that data brokers register with the California Attorney General (however, following amendments to the data broker registration law in late 2023, the data broker registration process and list is being transferred to the Agency). Under the law, a "data broker" is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. The terms "sell" and "personal information" are defined as set forth in the CCPA.

Oregon

In 2023, Oregon passed a law requiring data brokers register on an annual basis with the Department of Consumer and Business Services before collecting personal data in Oregon. Companies must register if they maintain data that is “categorized or organized for sale or licensing to another person.” The law took effect on January 1, 2024.

Texas

In 2023, Texas passed a law requiring data brokers register with the Secretary of State. The law has a narrower scope than most of the other state data broker registration laws in that it only applies to businesses that (1) in a 12-month period, derive more than 50% of their revenue from the processing or transfer of personal data that the business did not collect directly from individuals, or (2) derive revenue from the processing or transfer of personal data of more than 50,000 individuals whose data the business did not directly collect. The law took effect on September 1, 2023, with first registrations due March 1, 2024.

Vermont

In 2018, Vermont passed a law requiring data brokers to register with the Secretary of State and adhere to minimum data security standards. Under the law a “data broker” is defined as a company that collects computerized, personal information of Vermont residents with whom the company has no direct relationship, and either sell or licenses that information.

There is no registration required for Data Protection Officers in Laos, or for any legal entities or individuals with a national data protection authority, as the case may be in other jurisdictions.

In addition, several state laws require entities that engage in certain types of telemarketing activities to register with the state attorney general or other consumer protection agency.

DATA PROTECTION OFFICERS

With the exception of entities regulated by HIPAA, there is no general requirement to appoint a formal data security officer or data privacy officer.

Massachusetts and some other state laws and federal regulations, including the recently updated FTC Safeguards Rule (applicable to non-banking financial institutions), require organizations to appoint one or more employees to maintain their information security program.

COLLECTION & PROCESSING

US privacy laws and self-regulatory principles vary widely, but generally require that a notice be provided or made available pre-collection *(eg,* in a privacy policy) that discloses a company's collection, use and disclosure practices, the related choices individuals have regarding their personal information, and the company's contact information.

Opt-in consent is required under certain circumstance to collect, use and disclose certain sensitive data, such as health information, credit reports, financial information, children’s personal information, biometric data, video viewing choices, geolocation data and telecommunication usage information.

All states with comprehensive privacy laws, other than California, Florida, Iowa, and Utah require a business obtain consent from consumers to collect their sensitive data. California requires businesses to provide individuals a right to limit use of their sensitive data, and Iowa and Utah require individuals be provided a notice and right to opt-out of the collection of sensitive data.

The (federal) Children’s Online Privacy Protection Act (COPPA) requires verifiable parental consent prior to the collection of any personal information from children under 13. In addition, the CCPA requires that a business obtain explicit consent prior to the sale of any personal information about a consumer that the business has "actual knowledge" is less than 16 years old, and where the consumer is less than 13 years old, express parental authorization is required. (As

DATA PROTECTION OFFICERS

Under the Law on Electronic Data Protection, there is no data protection officer so to speak. The law introduces the idea that a team or an employee is required to supervise the protection of sensitive data; no information is provided on the duties and rights of such team or employee, or their scope of work. Moreover, the team or employee in charge of the protection of sensitive data is not required to register with any authority.

COLLECTION & PROCESSING

The collection of information is defined under the Instructions on the Implementation of the Law on Electronic Data Protection as “*the compiling of information in a database...for the convenience of access, monitoring, and use*...”.

The Law on Electronic Data Protection speaks literally of “administration” of data. Administration of electronic data refers to the management and arrangement of data, which includes the collection, copying, submission, receipt, maintenance, and destruction of electronic data. This administration of data is carried out by the Data Administrator, which is defined as an “individual, legal entity, or organization which has the duty to administrate electronic data, such as: a Ministry, an Internet Data Center, a Telecommunications Service Provider, an Internet Service Provider, or a Bank.” Apart from this definition, and the examples provided in the law, the Lao regulatory framework does not provide official guidance on who may or may not fall under the definition of Data Administrator.

By law, all data, general or sensitive, requires consent from the Information Owner to be collected. However, there is no information on how this consent may be collected.

Information Owner is defined as the individual, legal entity, or organization who / which is the owner of the electronic data. In this regard, the law does not necessarily identify the Information Owner as an individual only, or an individual who may be identified

discussed further below, the definition of "sale" under the CCPA is very broad and may include online advertising and retargeting activities, for example.). Amendments to the CCPA expanded this concept to include “ sharing” of a minor’s personal information (meaning the disclosing of personal information for purposes of cross-contextual behavioral advertising).

Further, companies generally need to obtain opt-in consent prior to using, disclosing or otherwise processing personal information in a manner that is materially different than what was disclosed in the privacy policy applicable when the personal information was initially collected. The FTC deems such changes ‘ retroactive material changes’ and considers it unfair and deceptive to implement a retroactive material change without obtaining prior, affirmative consent. Under the CCPA, which applies to individual and household data about California residents, businesses must, among other things:

- At or before collection, provide a notice to consumers disclosing the categories of personal information to be collected. the purposes for collecting such information, whether such information will be sold or shared, and how long such information will be retained or the criteria to determine such period.
- Post a privacy policy that discloses
    - the categories of personal information collected, categories of personal information disclosed for a business purpose, and categories of personal information "sold" and "shared" by the business in the prior 12 months
    - the purposes for which the business collects, uses, sells, and shares personal information
    - the categories of sources from which the business collects personal information
    - the categories of third parties to whom the business discloses personal information and
    - the rights consumers have regarding their personal information and how to exercise those rights
- Include a “do-not-sell-or-share my information” link on the business's website and page where consumers can opt-out of the sale and sharing of their personal information (if applicable)
- Generally, provide at least two methods for consumers to submit CCPA requests to the

according to personal data that relates to him / her. The law only provides that the Information Owner is the entity that “owns” the information.

Sensitive data is more regulated as it requires the approval from the Information Owner for the access, use, and disclosure of sensitive data. At the time of the collection, the Information Owner must be informed of:

- the identity of the Data Administrator;
- the purpose of the collection of the information;
- the type of information that will be collected;
- the rights of the Information Owner, which include:
    - the right to amend the information provided;
    - the right to stop the sending or transfer of information to third parties;
    - the right to delete the information collected per request, or at the time that the purpose of the collection of the information expires.

Also, the Data Administrator and the Information Owner have the duty to ensure that the information provided is correct — it does not contravene local regulations, and does not affect the country’s socio-economic development, national stability, or social order.

business, including an online method (e.g., submission of an online form) and a toll-free number

Other California privacy laws (*eg*, the California “ Shine the Light Law” and the California Online Privacy Protection Act) currently in force impose additional notice obligations, including:

- Where any personal information is disclosed to a third party for their own marketing use, a specific notice about such disclosure (*eg*, in a company’s privacy policy) must be provided and accessible through a special link on their homepage. Further, the law gives California residents to request a list of the personal information and third parties to whom such information was disclosed for marketing purposes in the prior 12 months
- Whether the company honors any do-not-track mechanisms

Under the comprehensive US state privacy laws , individuals have various qualified rights to request access to, correction, and deletion of their personal information and to “opt out” of sales, sharing, and the use of their personal information for targeted advertising purposes. Further, these laws require businesses to conduct data protection or risk assessments before engaging in certain higher-risk processing activities, such as processing that relates to:

- Certain unfair or intrusive profiling or targeted advertising purposes
- Selling of personal data
- Processing sensitive data

All states other than California and Utah require businesses to establish an internal process whereby consumers may appeal a controller’s refusal to take action on a privacy request and, where the appeal is denied, a method by which the consumer can submit a complaint to the state’s Attorney General.

Other states impose a wide range of specific requirements, particularly in the student and employee privacy areas. For example, a significant number of states have enacted employee social media privacy laws, and, in 2014 and 2015, a disparate array of education privacy laws. In addition, there are several sector-specific privacy laws that impose notice obligations, significantly limit permitted disclosures of personal information, and grant individuals the right to access or review records about the individual that are held by the regulated entity.

The US also regulates marketing communications extensively, including telemarketing, text message marketing, fax marketing and email marketing (which is discussed below).

TRANSFER

There are generally no geographic transfer restrictions that apply in the US, except regarding the storing of some governmental records and information. However, the HIPAA Privacy Rule requires that covered entities not disclose protected health information outside the US without appropriate safeguards.

TRANSFER

The Law on Electronic Data Protection provides that the transfer of data must abide by the following requirements:

- the Information Owner has given its consent for the transfer of the electronic data, and the individual or legal entity;
- transferring the electronic data ensures that the receiving entity can protect the electronic data properly;
- documents concerning important information, such as financial, banking, investment, and accounting information, must be encrypted;
- information which is transferred or submitted must not be distorted;
- the transfer must be in line with the agreement between the sender and the recipient; and
- submission or transfer of data must be stopped when the receiver of the data does not intend to receive the information anymore.

The law does not address whether the requirements above should be applied to all individuals or entities, or only to the Data Administrator.

In addition, the Law on Electronic Data Protection emphasizes that any individual, legal entity, or organization contemplating sending or transferring personal data or official data (pertaining to governmental bodies) out of Laos must obtain the consent of the Data Administrator, and ensure that such submission or transfer does not contravene the Lao laws without further details.

SECURITY

Most US businesses are required to take reasonable technical, physical and organizational measures to protect the security of sensitive personal information (*eg,* health or financial information, telecommunications usage information, biometric data, or information that would require security breach notification). A few states have enacted laws imposing more specific security requirements for such data.

SECURITY

Generally, the Law on Electronic Data Protection requires the Data Administrator to ensure the following regarding the storage / maintenance of electronic data:

- there is a team or employee responsible for the administration of sensitive data;
- there is, among other things, an adequate system to store or use the data, and a data safeguard system to protect the data;

For example, Massachusetts has enacted regulations that apply to any company that collects or maintains sensitive personal information (eg, name in combination with Social Security number, driver's license, passport number, or credit card or financial account number) on Massachusetts residents. Among other things, the Massachusetts regulations require regulated entities to have a comprehensive, written information security program and set forth the minimum components of such program, including binding all service providers who touch this sensitive personal information to protect it in accordance with the regulations. Massachusetts law includes encryption requirements on the transmission of sensitive personal information across wireless networks or beyond the logical or physical controls of an organization, as well as on sensitive personal data stored on laptops and portable storage devices.

Some states impose further security requirements on payment card data and other sensitive personal information. In 2019, New York passed a new law (the New York “SHIELD Act”) setting forth minimum security obligations for safeguarding private information. The SHIELD Act does not mandate specific safeguards but rather provides that a business will "be deemed to be in compliance" with the law if it implements a security program that includes elements set forth in the SHIELD Act.

The CCPA and Washington’s MHMD Act provide a private right of action to individuals for certain breaches of unencrypted personal information or consumer health data, respectively, which increases class action risks posed by data breaches.

There are also several other sectoral data security laws and regulations that impose specific security requirements on regulated entities – such as in the financial, insurance and health sectors. Federal financial regulators impose extensive security requirements on the financial services sector, including requirements for security audits of all service providers who receive data from financial institutions. For example, the New York Department of Financial Services (NYDFS) regulations impose extensive cybersecurity and data security requirements on licensees of the NYDFS, which includes financial services and insurance companies. The federal Gramm-Leach-Bliley Act and implementing rules and regulations require financial institutions to implement reasonable security measures.

HIPAA regulated entities are subject to much more extensive data security requirements. HIPAA security

- there is a backup system for destroyed or deleted data;
- information is recorded by way of another appropriate method (e.g. paper, magnetic storage), and the appropriate measure is used to guarantee good maintenance;
- a risk assessment is conducted on the protection system at least once a year, and any failures uncovered during the inspection are corrected;
- access to the system is inspected, and protected from any intrusion, virus, or other risks;
- any adverse events that have occurred or are about to occur are immediately solved; and
- the information that is under the responsibility of the Data Administrator is protected.

regulations apply to so-called ‘covered entities’ such as doctors, hospitals, insurers, pharmacies and other healthcare providers, as well as their ‘business associates’ which include service providers who have access to, process, store or maintain any protected health information on behalf of a covered entity. ‘Protected health information’ under HIPAA generally includes any personally identifiable information collected by or on behalf of the covered entity during the course of providing its services to individuals.

Internet of Things

California enacted the first US Internet of Things (IoT) legislation, effective January 1, 2020. Under SB 327, manufacturers of most IoT and Bluetooth connected devices will be required to implement reasonable security features ‘appropriate to the nature and the function of the device and the information the device may collect, contain or transmit’ and ‘designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.’ To the extent a device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature if (i) the preprogrammed is unique to each device manufactured, or (ii) the device forces the user to set a unique password upon first use.

BREACH NOTIFICATION

All 50 US states, Washington, DC, and most US territories (including, Puerto Rico, Guam and the Virgin Islands) have passed breach notification laws that require notifying state residents of a security breach involving more sensitive categories of information, such as Social Security numbers and other government identifiers, credit card and financial account numbers, health or medical information, insurance ID, tax ID, birthdate, as well as online account credentials, digital signatures and/or biometrics.

Under many state laws, where more than 500 individuals are impacted, notice must also be provided to credit bureaus. Nearly half of states also require notice to state Attorneys General and / or other state officials of certain data breaches. Further, certain states require impacted individuals to be provided with credit monitoring services for specified lengths of time if the breach involved Social Security numbers. Finally, some state data breach laws impose certain (varying) notice content and timing

BREACH NOTIFICATION

There is no mandatory breach notification in Laos under the Law on Electronic Data Protection. Individuals and legal entities facing a breach may make a notification, but to seek assistance and recommendations on how to solve the breach, and not for the sake of transparency.

However, in 2020, the Bank of Lao PDR issued the Decree on Consumer Protection Concerning Financial Services. Like the Law on Commercial Banks, enacted in 2018, the decree reiterates the importance of financial service providers (e.g. commercial banks) protecting their customer’s confidential information. However, unlike the Law on Commercial Banks, the Decree does mention a duty to maintain the confidentiality of “ personal information”.

The Decree provides that in the event that information relating to customers is breached, the financial service provider has an obligation to record the incident and immediately notify the affected customers. No details are

requirements with respect to notice to individuals and to state Attorneys General and/or other state officials.

Federal laws require notification in the case of breaches of healthcare information, breaches of information from financial institutions, breaches of telecom usage information held by telecommunication providers, and breaches of government agency information.

ENFORCEMENT

Various entities enforce US national and state privacy laws. Violations of privacy laws and rules are generally enforced by the FTC, state Attorneys General, or the regulator for the industry sector in question. Civil penalties can be significant, particularly for uncooperative or repeat offenders.

In addition, individuals may bring private rights of action (and class actions) for certain privacy or security violations.

Some privacy laws (for example, credit reporting, marketing and electronic communications, video viewing history, call recording and cable communications privacy laws) may be enforced through private rights of action, which give rise to class action lawsuits for significant

provided on what specifically must be recorded or notified. Likewise, the language used in the original document does not provide any assistance in interpreting the meaning of the term “affected.” The term for “affected” that is used in the Lao language version of the Decree is a term that is normally used to denote persons who have suffered negative consequences or damage from an act. In the event that the breach of information causes an important adverse impact, or if there is a large-scale breach, a report must be submitted to the Bank of Lao PDR. However, there is no definition of “important adverse impact” or “large scale breach.” Moreover, no specific sanction is provided for failing to submit the report.

The Law on Electronic Data Protection does not provide sanction for breach of the notification obligation. On the other hand, the Penal Code provides that any person disclosing the private confidential information of another person during the performance of their profession or duties, and who causes damages to the other person, will be liable to imprisonment of a term of three to six months and a fine between LAK 3 million (approx. USD 145) and LAK 10 million (approx. USD 480). However, Penal Code does not define “private confidential information”, nor does it state whether the disclosure of information must be intentional. To date, there is no official guidance clarifying whether the Penal Code applies to scenarios where customer data is breached as a result of a technical failure or other such incidents.

ENFORCEMENT

The enforcing authorities with regard to electronic data protection are:

- Ministry of Technology and Communications (MTC);
- Economic Police; and
- Lao People’s Court.

The Department of Cyber Security does not have by law the authority to issue fine or sanctions.

statutory damages and attorney’s fees, and individuals may bring actions for actual damages from data breaches.

The CCPA provides individuals with a private right of action and statutory damages, in the event of certain breaches of unencrypted personal information, where a business has failed to implement reasonable data security procedures (this applies to most categories of personal information under California’s breach notification law) – this raises significant class action risks. Currently, no other comprehensive state privacy laws contain a private right of action.

In June 2018, Ohio became the first US state to pass cybersecurity safe harbor legislation. Under SB 220, a company that has suffered a data breach of personal information has an affirmative defense if it has ‘ created, maintained, and complied with a written cybersecurity program that contains administrative, technical, and physical safeguards to protect personal information that reasonably conforms to an industry recognized cybersecurity framework’ (*e.g.*, PCI-DSS standards, NIST Framework, NIST special publications 800-171, 800-53, and 800-53a, FedRAMP security assessment framework, HIPAA, GLBA).

ELECTRONIC MARKETING

The US regulates marketing communications extensively, including email and text message marketing, as well as telemarketing and fax marketing.

Email

The CAN-SPAM Act is a federal law that applies labeling and opt-out requirements to all commercial email messages. CAN-SPAM generally allows a company to send commercial emails to any recipient, provided the recipient has not opted out of receiving such emails from the sender, the email identifies the sender and the sender’s contact information, and the email contains instructions on how the recipient can easily and without cost opt out of future commercial emails from the sender. The FTC and state Attorneys General, as well as ISPs and corporate email systems can sue violators. Knowingly falsifying the origin or routing of a commercial email message is a federal crime.

Text Messages

Federal and state regulations apply to the sending of marketing text messages to individuals. Express consent is

ELECTRONIC MARKETING

The Decision on Protection of Consumers Using Telecommunications and Internet Services (2020) regulates unsolicited commercial communications (e.g. phone calls or messages) to consumers, with the following restrictions:

- such calls and messages are prohibited from 8:00 to 17:00, Monday to Friday
- no more than 10 unsolicited commercial communications are allowed per month, per individual
- no more than two unsolicited commercial communications are allowed per day

The decision provides that any individual or legal entity intending to use unsolicited commercial communications for their goods or services must receive the consent of the telecommunications or internet service provider of the prospects they plan to call. The decision does not offer guidance on how the relevant service provider’s consent may be obtained. Rather, the decision requires the telecommunications and internet service providers to ensure that unsolicited

required to send text messages to individuals, and, for marketing text messages, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any text messaging (marketing or informational) program needs to be carefully reviewed for strict compliance with legal requirements.

Calls to Wireless Phone Numbers

Similar to text messages, federal and state regulations apply to marketing calls to wireless phone numbers. Prior express consent is required to place phone calls to wireless numbers using any autodialing equipment, and, for marketing calls, express written consent is required (electronic written consent is sufficient, but verbal consent is not). The applicable regulations also specify the form of consent. This is a significant class action risk area, and any campaign or program that involves calls (marketing or informational) to phone numbers that may be wireless phone numbers needs to be carefully reviewed for strict compliance with legal requirements. The definition of autodialing equipment is generally considered to, broadly, include any telephone system that is capable of (whether or not used or configured storing or producing telephone numbers to be called, using a random or sequential number generator.

Telemarketing

Beyond the rules applicable to text messaging and calling to wireless phone numbers, there are federal and state telemarketing laws as well. Federal telemarketing laws apply to most telemarketing calls and programs, and state telemarketing law will apply to telemarketing calls placed to or from within that particular state. As a result, most telemarketing calls are governed by federal law, as well as the law of one or more states. Telemarketing rules vary by state, and address many different aspects of telemarketing, such as calling time restrictions, do-not-call registries, opt-out requests, mandatory disclosures, requirements for completing a sale, executing a contract or collecting payment during the call, further restrictions on the use of auto-dialers and pre-recorded messages, and record-keeping requirements. Many states also require telemarketers to register or obtain a license to place telemarketing calls.

Fax Marketing

Federal law and regulations generally prohibit the sending of unsolicited advertising by fax without prior, express

communication commercials are made by authorized persons. In addition, the decision delegates these providers to monitor the distribution of unsolicited commercial messages, thereby ensuring that these limits are not breached.

Consumers who receive unsolicited commercial communications can file a complaint with the MPT and resolve subsequent disputes with the relevant service provider. The decision also notes that consumers can voice complaints or seek guidance via one of the following official hotlines:

- 1510 – Ministry of Industry and Commerce
- 1516 – Prime Minister’s Office
- 156 – National Assembly

The Ministry of Industry and Commerce’s website is also expected to become an available channel for complaints in the future.

consent. Violations of the law are subject to civil actions and have been the subject of numerous class action lawsuits. The law exempts faxes to recipients that have an established business relationship with the company on whose behalf the fax is sent, as long as the recipient has not opted out of receiving fax advertisements and has provided their fax number ‘voluntarily,’ a concept which the law specifically defines.

The law also requires that each fax advertisement contain specific information, including:

- A ‘clear and conspicuous’ opt-out method on the first page of the fax
- A statement that the recipient may make a request to the sender not to send any future faxes and that failure to comply with the request within 30 days is unlawful, and
- A telephone number, fax number, and cost-free mechanism to opt-out of faxes, which permit consumers to make opt-out requests 24 hours a day, seven days a week
- Violations are subject to a private right of action and statutory damages, and thus pose a risk of class action lawsuits

ONLINE PRIVACY

There is no specific federal law that *per se* regulates the use of cookies, web beacons and other similar tracking mechanisms. However, the state online privacy laws require notice of online tracking and of how to opt out of it.

Under California law, any company that tracks any personally identifiable information about consumers over time and across multiple websites must disclose in its privacy policy whether the company honors any ‘ Do-Not-Track’ method or provides users a way to opt out of such tracking. The same law also requires website operators to disclose in their privacy policy whether any third parties may collect any personally identifiable information about consumers on their website and across other third party websites, and prohibits the advertising of certain products, services and materials (including alcohol, tobacco, firearms, certain dietary supplements, ultraviolet tanning, tattoos, obscene matters, etc.). Further, under most of the comprehensive state laws, information collected via cookies, online, mobile and targeted ads, and other online tracking are subject to the requirements of the law.

ONLINE PRIVACY

As provided, the collection of data must receive the consent of the relevant Information Owner.

On the other hand, based on the main laws and regulations above, it is difficult to anticipate the category of data cookies and location data according to the ambiguous definitions of general data, sensitive data, and personal data.

Further, given the broad definition of personal information under the comprehensive state privacy laws, information collected via cookies and similar technologies is generally subject to the requirements of the law (e.g., notice and consumer rights). For example, under the CCPA a 'sale' includes selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer’s personal information by one business to another business or a third party for monetary or other valuable consideration. ‘Sharing’ under the CCPA is defined as sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged. These broad definitions sweep in certain online advertising activities -- for example, where a business permits the collection and use of information through certain third party cookies and tags on their website, in order to better target the business' ad campaigns on third party websites or in exchange for compensation from a third party ad network.

Universal Opt-Out Signals / Global Privacy Control (GPC)

Amendments to the CCPA, and recent enforcement actions by the California Attorney General, have highlighted the requirement that businesses that process personal information for targeted advertising purposes allow consumers to opt-out of sales and sharing, using an opt-out preferences signal sent by the consumer’s browser or a browser plugin, aso referred to as Global Privacy Control (GPC). Colorado’s comprehensive privacy law introduces the same requirement, with an effective date of July 1, 2024.

Minors

The Children’s Online Privacy Protection Act and regulations (COPPA) applies to information collected automatically (*eg*, via cookies) from child-directed websites and online services and other websites, online services and third party ad networks or plug-ins that knowingly collect personal information online from children under 13. COPPA also regulates behavioral advertising to children under 13 as well as the collection of geolocation information, requiring prior verifiable

parental consent to engage in such advertising or collection.

California law requires that operators of websites or online services that are directed to minors or that knowingly collect personally identifiable information from minors permit minors that are registered users of their sites to remove any content the minor has posted from the site or online service. The law does not give minors the right to remove information posted by third parties. Minors must be given clear notice on how to exercise their right to removal. Certain state privacy laws (such as the CCPA, CPA or VCDPA) also require that a business obtain explicit consent prior to selling any personal information about an individual the business has actual knowledge is under 16 years old.

Location Data

Generally, specific notice and consent in needed to collect precise *(e.g.,* mobile device) location information. The CCPA defines precise geolocation information as “any data derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet.” Connecticut and Utah law carry similar definitions, albeit with a radius of 1,750 feet.

KEY CONTACTS

Kate Lucente
Partner and Co-Editor, Data Protection Laws of the World
T +1 813 222 5927
kate.lucente@dlapiper.com

Andrew Serwin
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +1 858 677 1418
andrew.serwin@dlapiper.com

Jennifer Kashatus
Partner
T +1 202 799 4448
jennifer.kashatus@dlapiper.com

KEY CONTACTS

Dino Santaniello
Head of Office
Tilleke & Gibbins Lao Co., Ltd
T +856 21 262 355
dino.s@tilleke.com

Saithong Rattana
Attorney-at-Law
Tilleke & Gibbins Lao Co., Ltd
T +856 21 262 355
saithong.r@tilleke.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.