DATA PROTECTION LAWS OF THE WORLD

Singapore vs United States

DLA PIPER

SINGAPORE

Last modified 20 December 2023

LAW

Singapore enacted the Personal Data Protection Act of 2012 (No. 26 of 2012) on October 15, 2012, and it was subsequently amended / enhanced via the Personal Data Protection (Amendment) Act 2020 (together, the “ **Act**”).

The Act has extraterritorial effect, meaning it applies to organizations collecting, using or disclosing personal data in Singapore whether or not the organization itself has a physical presence or is registered as a company in Singapore.

In addition to the Act, the Singapore data protection regime consists of various general or sector / industry-specific guidelines issued by the Personal Data Protection Commission (“**Commission**”). While these guidelines are advisory in nature and not legally binding, they indicate the manner in which the Commission will interpret the Act. Therefore, it is best practice to carefully observe and follow these guidelines.

The data protection obligations under the Act do not apply to the public sector, to whom separate rules under the Government Instruction Manual 8 (“**IM8** ”) and the Public Sector (Governance) Act apply. Collectively, these rules provide comparable standards of data protection compared to the Act, including similar investigations and enforcement actions taken against data security breaches. The Public Sector Data Security Review Committee was convened on March 31, 2019 to conduct a comprehensive review of data security policies and practices across the public sector. The Government implemented its recommendations and adopted changes to its data security measures. Examples include:

- Requiring officers to password-protect files containing sensitive data when sending out; and
- Enhancing the data incident management framework with standardized process to notify affected individuals in data incidents and conduct post-incident inquiry.

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

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

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/w

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

DEFINITIONS

Definition of personal data

Personal data is defined in the Act to mean data, whether true or not, about an individual (whether living or recently deceased*) who can be identified from:

- that data; or
- that data and other information to which the organization has, or is likely to have access.

*The Act's application to recently deceased individuals is limited to disclosure and protection of personal data where such data is about an individual who has been deceased for ten years or fewer.

The data protection obligations under the Act do not apply to business contact information. This excludes from the Act the following if provided solely for business purposes:

- Name
- Position name or title
- Business telephone number
- Business address
- Business electronic mail address
- Business fax number

It is important to note that the Act still governs business contact information provided by individuals solely in their personal capacity. Where the purposes of provision of business contact information are mixed (that is, for both business and personal purposes), the Act does not apply.

Definition of sensitive personal data

There is no definition of sensitive personal data in the Act.

However, non-binding guidance from the Commission indicates that sensitivity of data is a factor for consideration in implementing policies and procedures to ensure appropriate levels of security for personal data. For example, encryption is recommended for sensitive data stored in an electronic medium that has a higher risk of adversely affecting the individual should it be compromised. Where any personal data collected is particularly sensitive (e.g. regarding physical or mental health), as a matter of best practice, such data should only be used for limited purposes and the security measures afforded to such data should take into account the sensitivity of the data.

In addition, the non-binding guidelines issued by the Commission also provide that, in its calculation of financial

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.

Generally, includes personal health data, financial data, credit worthiness data, student data, biometric data, personal information collected online from children under

penalties for breaches of the Act, the Commission would consider whether the organization in question is in the business of handling large volumes of sensitive personal data, the disclosure of which may cause exceptional damage, injury or hardship to an individual (such as medical or financial data), but it has failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of such personal data.

The Commission has also issued a set of advisory guidelines to impose restrictions on the collection, use and disclosure of National Identification Registration Card (“**NRIC**”) numbers, due to the sensitive nature of the information contained in NRICs (and other similar forms of identification). Organizations are not permitted to collect either the NRIC number or the physical cards or other similar forms of identification unless the organization is permitted to do so under the law or if the collection is necessary for the verification of an individual's identity to “high degree of fidelity” (where it is extremely important the individual’s identity is verified, and failure to do so may, for example, pose a significant safety or security risk).

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

Personal Data Protection Commission

Address

10 Pasir Panjang Road #03-01
Mapletree Business City
Singapore 117438

Telephone

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 enforce federal privacy regulations (including telemarketing, email marketing, and children's privacy) and

+65 6377 3131

Fax

+65 6577 3888

Email

info@pdpc.gov.sg

Website

www.pdpc.gov.sg

REGISTRATION

There are no registration requirements under the Act.

While not a requirement, the Commission strongly encourages organizations to register their Data Protection

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

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

Officers ("**DPOs**") with the Commission via the Commission's website, to assist DPOs in keeping up to date with developments in the law. Organisations may also choose to register their DPOs’ business contact information as part of their Accounting and Corporate Regulatory Authority (“**ACRA**”) Bizfile details, so that these will show up in search results on the ACRA website.

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.

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

It is mandatory for each organization to appoint one or more DPOs to be responsible for ensuring the organization’s compliance with the Act. An organization may appoint one person or a team of persons to be its DPO. Once appointed, the DPO may in turn delegate certain responsibilities, including to non-employees of the organization. The business contact information of the DPO must be made available to the public.

While there is no requirement for the DPO to be a citizen or resident in Singapore, the Commission suggests that the DPO should be readily contactable from Singapore, available during Singapore business hours and, where telephone numbers are provided, these should be Singapore telephone numbers.

Failure to appoint a DPO may lead to a preliminary investigation by the Commission. If an organization or an individual fails to cooperate with the investigation, this will constitute an offence. As a result, an individual may be subject to a fine of up to SGD 10,000 or imprisonment for a term not exceeding 12 months, or to both. An organization may be subject to a fine of up to SGD 100,000.

COLLECTION & PROCESSING

Organizations may only collect, use or disclose personal data in the following scenarios:

- They obtain express consent from the individual prior to the collection, use, or disclosure of the personal data (and such consent must not be a condition of providing a product or service, beyond what is reasonable to provide such product or service; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices), and have also provided the relevant data protection notice (notifying purposes of collection, use and disclosure) to the individual before, or at the time when they are collecting, using or disclosing the personal data. It is also possible to obtain the deemed consent of the individual to the collection, use, or disclosure of the personal data in accordance with the relevant conditions of the Act (see the Personal Data Protection Regulations 2021).
- Where the limited specific exclusions prescribed

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.

in the Act apply (if no consent or deemed consent is given). Such exclusions include vital interests of individuals, matters affecting public, legitimate interests, business asset transactions, business improvement purposes and other additional bases.

The Act currently in force expanded the concept of “deemed consent” to cover circumstances where: (i) the collection, use or disclosure of personal data is reasonably necessary to conclude or perform a contract or transaction; or (ii) (a) where individuals have been notified of the purpose of the intended collection, use or disclosure of personal data, given a reasonable opportunity to opt-out, and have not opted out, and (b) the organization has conducted an assessment on the likely adverse effect on such individuals, and identified and put in place reasonable measures to eliminate, reduce the likelihood of or mitigate any such adverse effect.

An individual may at any time withdraw any consent given, or deemed given under the Act, upon giving reasonable notice to the organization.

Further, any collection, use or disclosure of the personal data must only be for the purposes that a reasonable person would consider appropriate in the circumstances, and for purposes to which the individual has been notified of. Such notification must be made in accordance with the requirements of the Act.

An organization must also do all of the following:

- Make information about its data protection policies, practices and complaints process publicly available.
- Cease to retain personal data or anonymize it where it is no longer necessary for any business or legal purpose. Ensure personal data collected is accurate and complete if likely to be used to make a decision about the individual or disclosed.
- Respond to requests by data subjects under their statutory rights, including a new right of data portability (this right is expected to come into force soon).

Data intermediaries that process personal data on behalf of another organization (i.e. data controller) pursuant to a written contract are exempt from most of the data protection obligations under the PDPA. However, data intermediaries are directly liable under two specific obligations relating to the retention (see above) and protection (see Security) of personal data.

Data protection management program (“**DPMP**

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 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

”) and data protection impact assessment (“ **DPIA**”) guides were published by the Commission in November 2017 and updated in September 2021.

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 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

TRANSFER

In disclosing or transferring personal data to onshore third parties (including affiliates), an organization should ensure that it has obtained the individual's deemed or express consent to such transfer (unless exemptions apply) and, if this was not done at the time the data was collected, additional consent will be required (unless exemptions apply).

It is also a requirement under the Act for organizations to enter into written agreements with their data intermediaries to whom they transfer personal data and who process such data on behalf of the organizations.

The Act also contains offshore transfer restrictions, which require an organization to ensure that the receiving organization has in place "comparable protection" to the standards set out in the Act when transferring personal data outside of Singapore. Mechanisms to achieve this include (this is not a comprehensive list): data transfer agreements (for which the Commission has released suggested sample clauses); the individual has given consent (provided required notices have been given to the individual setting out the basis upon which their data will be protected in the country or territory to which their personal data will be transferred); and where transfers are considered necessary in certain prescribed circumstances (which include in connection with performance of contracts between the transferring organization and the individual, subject to certain conditions being met). An organization may apply to be exempted from any requirement prescribed under the Act in respect of any transfer of personal data out of Singapore. An exemption may be granted on such conditions as the Commission may require.

The Amendment Act provides for a new right of data

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.

portability on electronic data (this right is expected to come into force soon). Individuals may request an organization (“**Porting Organization**”) to transmit certain data about them to another organization. The Porting Organization must have an ongoing relationship with the individual, and have collected or created such data.

The Commission has published guides to data sharing (covering intragroup and third party sharing) with practical nonbinding guidance on data transfer / sharing for organizations, as well as DPMP and DPIA guides (see Collection & Processing).

SECURITY

Organizations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, the loss of any storage medium or device on which personal data is stored, or similar risks. Data intermediaries are also directly liable and subject to the same security obligation. The Act does not specify security measures to adopt and implement, however the Commission has issued best practice guidance which provides specific examples, including with respect to cloud computing and IT outsourcing.

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.

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 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

Under the current Act, where an organization has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, it must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a “notifiable data breach” (as defined in the current Act). A data breach means (a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data, or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur. A data breach constitutes a “notifiable data breach” if:

i. it results in, or is likely to result in, significant harm to the affected individuals (including one that compromises personal data prescribed under the Personal Data Protection (Notification of Data Breaches) Regulations 2021); or
ii. it is of a significant scale (i.e. one that affects 500 or more individuals).

An organization must notify the Commission as soon as practicable and in any case no later than three calendar days after the day the organization makes the above assessment of a notifiable data breach. If the data breach results in, or is likely to result in, significant harm to the affected individual(s), an organization must also notify each affected individual in any manner that is reasonable in the circumstances.

The Personal Data Protection (Notification of Data Breaches) 2021 sets out the list of information to be included in notifications to the Commission and affected individuals.

Where a data breach is discovered by a data intermediary, the data intermediary must notify the organization (i.e. data controller) without undue delay from the time the data intermediary has credible grounds to believe that a data breach has occurred in relation to personal data that it is processing on behalf of and for the purposes of the organization. Upon notification by the data intermediary, the organization must conduct an assessment of whether the data breach is a notifiable data breach.

In addition, the Cybersecurity Act 2018 (“**CSA** ”) was passed in Singapore in early 2019. The CSA primarily contains obligations applicable to organizations which have been designated as owners of critical

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 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.

information infrastructure. In particular, if your organization has been designated by the Cybersecurity Commissioner as the owner of a critical information infrastructure, additional obligations will apply to your organization in relation to data breach incident handling and notification. Amendments were proposed to the CSA in December 2023, with the Cybersecurity (Amendment) Bill (Bill) made available for public consultation until early January 2024. The Bill proposes imposing obligations on other operators of digital infrastructure and technology, to ensure that the CSA keeps pace with technological developments and industry practices.

ENFORCEMENT

Enforcement of the Act is carried out by the Commission, which include giving directions to an organization to do any of the following:

- Stop collection, use or disclosure of personal data in contravention of the Act;
- Destroy personal data collected in contravention of the Act;
- Provide or refuse access to or correction of personal data;
- Pay a financial penalty of either up to (i) 10% of an organization’s annual turnover in Singapore for those with annual turnover in Singapore that exceeds SGD 10 million, or (ii) SGD 1 million.

These directions may be registered with the Singapore District Courts so that they may have the force and effect of an order of court.

The Commission issued revised Advisory Guidelines on Enforcement Data Protection Provisions on 1 February 2021.

Further, new criminal offences are in force to hold individuals accountable for egregious mishandling of personal data, including knowing or reckless unauthorized disclosure, unauthorised re-identification of anonymized data, or use of personal data for a gain or to cause harm or loss to another person.

Guidelines published by the Commission indicate how in practice the Commission proposes to handle complaints, reviews and investigations of breaches of the data protection rules under the Act, and to approach enforcement and sanctions. Amongst other things, they set out the Commission's enforcement objectives, and guidance regarding the mitigating and aggravating factors

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 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

that the Commission will take into account when issuing directions and sanctions (for example, prompt initial response and resolution of incidents; cooperation with investigations; and breach notification). The Commission has in the past couple of years stepped up its efforts to enforce the Act, highlighting the growing risks of non-compliance with the Act in Singapore.

Directions or decisions given are subject to reconsideration by the Commission, upon written application by any aggrieved party.

Directions, decisions or reconsiderations of the Commission may also be subject to appeal to a Data Protection Appeal Committee, unless the direction or decision to be appealed is the subject of an application for reconsideration, in which case such appeal would be deemed withdrawn.

Directions may only be appealed to the High Court and Court of Appeal with regard to the following:

- A point of law arising from a direction or decision of the Appeal Committee
- Any direction of the Appeal Committee as to the amount of a financial penalty

Any person who has suffered loss or damage directly as a result of a contravention of the Act is also entitled to pursue a private action in court. However, where the Commission has made a decision with regard to the said loss or damage, a right of private action will only be possible after the decision has become final as a result of there being no further right of appeal. The court may grant to the plaintiff all or any of the following:

- Relief by way of injunction or declaration
- Damages
- Such other relief as the court thinks fit

ELECTRONIC MARKETING

The data protection principles in the Act apply to any marketing activities (including electronic marketing) which involve the collection, use or disclosure of personal data.

In addition, any organization or person that wishes to engage in any telemarketing activities will need to comply with the "Do Not Call" provisions under the Act. Generally, a person or organization who wishes to send marketing messages to a Singapore telephone number should first obtain the clear and unambiguous consent of the individual to the sending of the messages to such Singapore telephone number. The consent must:

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

- be evidenced in written or other form so as to be accessible for subsequent reference;
- not be a condition for supplying goods, services, land, interest or opportunity; and
- not be obtained through the provision of false or misleading information or through deceptive or misleading practices.

In the absence of such consent, organizations must check and ensure that the telephone number is not on a Do-Not-Call register maintained by the Commission (“DNC Register”). There are also other requirements, including a duty to identify the sender of the marketing message and provide clear and accurate contact information, as well as a duty not to conceal the calling line identity of any voice calls containing such marketing messages. An individual may at any time apply to the Commission to add or remove his Singapore telephone number on the DNC Register.

Further, the current Act provides the role of “checkers” which are entities that provide information for gain on whether a Singapore telephone number is listed in the DNC Register for the purposes of another organization’s obligations under the Act. It imposes obligations on third party checkers, and checkers will be liable for DNC infringements resulting from any erroneous information provided by them.

The Act will apply to marketing messages addressed to a Singapore telephone number in the following circumstances:

- The sender of the marketing message is present in Singapore when the message was sent.
- The recipient of the marketing message is present in Singapore when the message is accessed.

Electronic marketing activities are also regulated under the Spam Control Act 2007 (**"SCA"**), to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail or by SMS or MMS to a mobile telephone number.

The DNC provisions under the current Act include a prohibition on sending messages to telephone numbers generated or obtained through dictionary attacks (generating telephone numbers by combining numbers into numerous permutations) or address-harvesting software. Related amendments to the SCA to prohibit sending unsolicited electronic messages to instant messaging accounts are also in force.

The Commission issued the revised Advisory Guidelines

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

on the Do Not Call Provisions on February 1, 2021.

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 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

ONLINE PRIVACY

Currently, there are no specific requirements relating to online privacy (including cookies and location) under the Act. Nevertheless, an organization that wishes to engage in any online activity that involves the collection, use or disclosure of personal data will still need to comply with the general data protection obligations under the Act. For example, if an organization intends to use cookies to collect personal data, it must obtain consent before use of any such cookies. For details of the consent required, please see Collection & Processing. The Commission has published nonbinding guidelines providing practical tips on pertinent topics such as securing electronic personal data, building websites, the capture of IP addresses and the use of cookies.

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 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.

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

Carolyn Bigg
Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com

Yue Lin Lee
Senior Associate
T +852 2103 0890
yuelin.lee@dlapiper.com

DATA PRIVACY TOOL

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

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

DATA PRIVACY TOOL

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