DATA PROTECTION LAWS OF THE WORLD

Malaysia vs United States

DLA PIPER

MALAYSIA

Last modified 21 December 2020

LAW

Malaysia's first comprehensive personal data protection legislation, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010 and came into force on November 15, 2013.

As part of an ongoing review of the PDPA, the Personal Data Protection Commissioner of the Ministry of Communications and Multimedia Malaysia has issued Public Consultation Paper No. 01/2020 – Review of Personal Data Protection Act 2010 (PC01/2020) dated February 14, 2020 to seek the views and comments of the public on 22 issues set out in PC01/2020, some of which are set out below.

UNITED STATES

Last modified 28 January 2021

LAW

The US has several sector-specific and medium-specific national privacy or data security laws, including laws and regulations that apply to financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing.

The US also has hundreds of privacy and data security among its 50 states and territories, such as requirements for safeguarding data, disposal of data, privacy policies, appropriate use of Social Security numbers and data breach notification. California alone has more than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020, which will be substantially amended by the California Consumer Privacy Rights Act, which takes effective January 1, 2023. The CCPA applies cross-sector and introduces sweeping definitions and broad individual rights, and imposes substantial requirements and restrictions on the collection, use and disclosure of *personal information*, which is very broadly defined as explained later in this chapter. A number of other US states are also currently proposing and considering state-level privacy legislation; in general, such legislation is similar to the CCPA in some ways, but also includes some additional or materially different requirements. Thus, it is highly possible that additional state-level privacy laws will be enacted in the US that impose requirements that go beyond or are materially different from those of the CCPA. More information from DLA Piper on the CCPA and related issues is available at https://www.dlapiper.com/en/us/focus/ccpa/.

In addition, the US Federal Trade Commission (FTC) has jurisdiction over a wide range of commercial entities under its authority to prevent and protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices. The FTC uses this authority to, among other things, issue regulations, enforce certain privacy laws and take enforcement actions and investigate companies for:

- Failing to implement reasonable data security measures
- Making materially inaccurate privacy and security representations 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 the FTC's consumer privacy framework or certain national privacy laws and regulations

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.

DEFINITIONS

Definition of personal data

'Personal data' means any information in respect of commercial transactions that is:

- Being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose
- Recorded with the intention that it should wholly or partly be processed by means of such equipment, or
- Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, and, in each case

...that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user.

Personal data includes any sensitive personal data or expression of opinion about the data subject. Personal data does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010.

Definition of sensitive personal data

DEFINITIONS

Definition of personal data

Varies widely by regulation. The FTC now considers information that is linked or reasonably linkable to a specific individual, which could include IP addresses and device identifiers, as personal data.

The CCPA defines personal information as any 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. Under the law, consumer is broadly defined as any resident of California.

In contrast, state breach notification laws and data security laws typically define personal information more narrowly focusing on more sensitive categories of information, as described below.

Definition of sensitive personal data

'Sensitive personal data' means any personal data consisting of information as to the physical or mental health or condition of a data subject, his or her political opinions, his or her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him or her of any offense or any other personal data as the Minister of Communications and Multimedia (Minister) may determine by published order. Other than the categories of sensitive personal data listed above, the Minister has not published any other types of personal data to be sensitive personal data as of December 15, 2020.

NATIONAL DATA PROTECTION AUTHORITY

Pursuant to the PDPA, a Personal Data Protection Commissioner (Commissioner) has been appointed to implement the PDPA's provisions. The Commissioner will be advised by a Personal Data Protection Advisory Committee who will be appointed by the Minister, and will consist of one Chairman, three members from the public sector, and at least seven, but no more than eleven other members. The appointment of the Personal Data Protection Advisory Committee will not exceed a term of three years; however, members can be appointed for two successive terms.

The Commissioner's decisions can be appealed through the Personal Data Protection Appeal Tribunal. The following are examples of appealable decisions:

- Decisions relating to the registration of data users under Part II Division 2 of the PDPA
- The refusal of the Commissioner to register a code of practice under Section 23(5) of the PDPA
- The service of an enforcement notice under Section 108 of the PDPA
- The refusal of the Commissioner to vary or cancel an enforcement notice under Section 109 of the PDPA, or
- The refusal of the Commissioner to conduct or continue an investigation that is based on a complaint under Part VIII of the PDPA.

If a data user is not satisfied with a decision of the Personal Data Protection Advisory Committee, the data user may proceed to file a judicial review of the decision in the Malaysian High Courts.

Varies widely by sector and by type of statute.

Generally, 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.

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.

NATIONAL DATA PROTECTION AUTHORITY

No single national authority.

The FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (eg, for telemarketing, commercial email, 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. The California Attorney General has the authority to enforce the CCPA and most California consumer privacy laws.

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

Currently, the PDPA requires the following classes of data users to register under the PDPA:

1. **Communications**
    1. A licensee under the Communications and Multimedia Act 1998
    2. A licensee under the Postal Services Act 2012
2. **Banking and financial institution**
    1. A licensed bank and licensed investment bank under the Financial Services Act 2013
    2. A licensed Islamic bank and licensed international Islamic bank under the Islamic Financial Services Act 2013
    3. A development financial institution under the Development Financial Institution Act 2002
3. **Insurance**
    1. A licensed insurer under the Financial Services Act 2013
    2. A licensed takaful operator under the Islamic Financial Services Act 2013
    3. A licensed international takaful operator under the Islamic Financial Services Act 2013
4. **Health**
    1. A licensee under the Private Healthcare Facilities and Services Act 1998
    2. A holder of the certificate of registration of a private medical clinic or a private dental clinic under the Private Healthcare Facilities and Services Act 1998
    3. A body corporate registered under the Registration of Pharmacists Act 1951
5. **Tourism and hospitalities**
    1. A licensed person who carries on or operates a tourism training institution, licensed tour operator, licensed travel agent or licensed tourist guide under the Tourism Industry Act 1992
    2. A person who carries on or operates a registered tourist accommodation premises under the Tourism Industry Act 1992
6. **Transportation**
    1. Certain named transportations services providers
7. **Education**
    1. A private higher educational institution

REGISTRATION

There is no requirement to register databases or personal information processing activities.

- California: the CCPA (as amended in 2019) requires (subject to some exceptions) that data brokers register with the California Attorney General. 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.
- Vermont: in 2018, 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.

registered under the Private Higher Educational Institutions Act 1996
2. A private school or private educational institution registered under the Education Act 1996

8. **Direct selling**
    1. A licensee under the Direct Sales and Anti-Pyramid Scheme Act 1993
9. **Services**
    1. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961 carrying on business as follows:
        - legal
        - audit
        - accountancy
        - engineering
        - architecture
    2. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who conducts retail dealing and wholesale dealing as defined under the Control Supplies Act 1961
    3. A company registered under the Companies Act 1965 or a person who entered into partnership under the Partnership Act 1961, who carries on the business of a private employment agency under the Private Employment Agencies Act 1981
10. **Real estate**
    1. A licensed housing developer under the Housing Development (Control and Licensing) Act 1966
    2. A licensed housing developer under the Housing Development (Control and Licensing) Enactment 1978, Sabah
    3. A licensed housing developer under the Housing Developers (Control and Licensing) Ordinance 1993, Sarawak
11. **Utilities**
    1. Certain named utilities services providers
12. **Pawnbroker**
    1. A licensee under the Pawnbrokers Act 1972
13. **Moneylender**
    1. A licensee under the Moneylenders Act 1951

Certificates of registration are valid for at least one year, after which data users must renew registrations and may

not continue to process personal data.

Data users are also required to display their certificate of registration at a conspicuous place at their principal place of business, and a copy of the certificate at each branch, where applicable.

The Commissioner may designate a body as a data user forum for a class of data users. Data user forums can prepare codes of practice to govern compliance with the PDPA, which can be registered with the Commissioner. Once registered, all data users must comply with the provisions of the code, and non-compliance violates the PDPA. As of December 15, 2020, the Commissioner has published several codes of practice, including for the banking and financial sector, the aviation sector, the utilities sector, communications sector and the insurance and takaful industry in Malaysia.

DATA PROTECTION OFFICERS

Currently, Malaysian law does not require that data users appoint a data protection officer.

However, pursuant to PC01/2020, the Commissioner is considering introducing an obligation in the PDPA for a data user to appoint a data protection officer and to introduce a guideline pertaining to such appointments.

COLLECTION & PROCESSING

Under the PDPA, subject to certain exceptions, data users are generally required to obtain a data subject's consent for the processing (which includes collection and disclosure) of his or her personal data. Where consent is required from a data subject under the age of eighteen, the data user must obtain consent from the parent, guardian or person who has parental responsibility for the data subject. The consent obtained from a data subject must be in a form that such consent can be recorded and maintained properly by the data user.

Pursuant to PC01/2020, the Commissioner has sought feedback on its proposal to amend the General Principle provision to add clarity to the data subject's consent, whether it should be in a specific provision and the impact of having a default consent.

Malaysian law contains additional data protection

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 require organizations to appoint one or more employees to maintain their information security program.

Even so, appointing a chief privacy officer and a chief information security officer is a best practice which is common among larger organizations and increasingly also among mid-sized ones.

COLLECTION & PROCESSING

US privacy laws and self-regulatory principles vary widely, but generally requires 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 consumers have regarding their personal information, and the company's contact information.

Opt-in consent is generally required when personal information that is considered sensitive under US law is collected, used, and shared, such as health information, credit reports, financial information, student data, children's personal information, biometric data, video viewing choices, geolocation data and telecommunication usage information.

In addition, the CCPA requires that a business obtain explicit consent prior to the sale of any personal

obligations, including, for example, a requirement to notify data subjects regarding the purpose for which their personal data are collected and a requirement to maintain a list of any personal data disclosures to third parties.

On December 23, 2015, the Commissioner published the Personal Data Protection Standard 2015 ("Standards"), which set out the Commission's minimum requirements for processing personal data. The Standards include the following:

- Security Standard For Personal Data Processed Electronically
- Security Standard For Personal Data Processed Non-Electronically
- Retention Standard For Personal Data Processed Electronically And Non-Electronically
- Data Integrity Standard For Personal Data Processed Electronically And Non-Electronically

information about a consumer that the business has "actual knowledge" is less than 16 years old. (As discussed further below, the defnition of "sale" under the CCPA is very broad and may include online advertising and retargeting activities, for example.)

Further, companies generally need to obtain opt-in consent prior to using, disclosing or otherwise treating personal information in a manner that is materially different than what was disclosed in the privacy policy applicable when the personal information was 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 from all relevant individuals.

Under the CCPA (which applies to individual and household data about California residents, businesses must, among other things:

- At or before collection, notify individuals of the categories of personal information to be collected and the purposes of use of such information
- 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" by the business in the prior 12 months,
    - the purposes for which the business collects, uses and sells 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
- A "do-not-sell my information" link on the business's website and page where consumers can opt-out of the sale 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.

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 a number of 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).

Under the CCPA, prior to any sale of personal information, companies must provide individuals over 16 years old the right to opt-out, obtain prior consent from individuals ages 13 to 16, and obtain prior parental consent from individuals younger than 13. Sale is broadly defined to include selling, disclosing or granting access to personal information in exchange for any consideration or other thing of value. The CCPA also gives individuals broad access and data portability rights, as well as limited deletion rights and the right to obtain more detailed information about specific data collected, as well as disclosures of personal data by businesses.

TRANSFER

Under the PDPA, a data user may not transfer personal data to jurisdictions outside of Malaysia unless that jurisdiction has been specified by the Minister. However, there are exceptions to this restriction, including the following:

TRANSFER

No geographic transfer restrictions apply in the US, except with regard to storing some governmental records and information.

The US is a major point of storage of personal data. On July 16, 2020, the European Court of Justice—in its '

- The data subject has given his or her consent to the transfer.
- The transfer is necessary for the performance of a contract between the data subject and the data user.
- The data user has taken all reasonable steps and exercised all due diligence to ensure that the personal data will not be processed in a manner that would contravene the PDPA.
- The transfer is necessary to protect the data subject's vital interests.

In 2017, the Commissioner published a draft Personal Data Protection (Transfer of Personal Data to Places Outside Malaysia) Order 2017 to obtain public feedback on the proposed jurisdictions to which personal data from Malaysia may be transferred. As of December 15, 2020, the Minister has yet to approve the safe harbor jurisdictions. Once approved, a data user may transfer personal data to these safe harbor jurisdictions without having to rely on the data subject's consent or other prescribed exceptions under the PDPA.

Pursuant to PC01/2020, the Commissioner acknowledged that a clear provision and the conditions for transferring personal data to places outside Malaysia are essential to facilitate e-commerce transactions and free trade agreements, and opined that a whitelist appears to curb and set a barrier for data users to transfer personal data to places outside Malaysia. In view of this, the Commissioner is considering restructuring the provision on cross border transfers under the PDPA and removing the whitelist provision.

In addition, the Commissioner also acknowledged that data users with overseas branches may need to exchange information with its branches at some point. The Commissioner is considering issuing a guideline on the mechanism and implementation of cross border data transfer and has sought feedback on the important matters to be considered in the proposed guideline.

SECURITY

Under the PDPA, data users have an obligation to take 'practical' steps to protect personal data, and in doing so, must develop and implement a security policy. The Commissioner may also, from time to time, set out security standards with which the data user must comply, and the data user is required to ensure that its data processors comply with these security standards.

In addition, the Standards provide separate security

Schrems II' decision, invalidated the EU-US Privacy Shield program, finding that it does not provide adequate protection for personal data transferred from the EU to the US. Following the *Schrems II* decision, the Swiss Federal Data Protection and Information Commissioner (FDPIC) determined that the US-Swiss Privacy Shield fails to provide an adequate level of protection for personal data transferred from Switzerland to the United States, effectively invalidating the US-Swiss Privacy Shield Program.

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

standards for personal data processed electronically and for personal data processed non-electronically (among others) and require data users to have regard to the Standards in taking practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

Pursuant to PC01/2020, the Commissioner observed that there are many new technologies such as facial recognition and smart trackers being used as data collection endpoints, and thus is considering issuing a policy regarding the endpoint security which uses technologies such as encryption.

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 data 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 "SHEILD 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 provides a private right of action to individuals for certain breaches of unencrypted personal information, which has
greatly increased the class action posed by data breaches.

There are also a number of 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 national Gramm-Leach-Bliley Act and implementing 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

BREACH NOTIFICATION

There is no requirement under the PDPA for data users to notify authorities regarding data breaches in Malaysia. However, news reports dated October 5, 2018 suggest that Malaysia's laws could be updated, to include data breach notification requirements modeled after those under the European Union's General Data Protection Regulation (GDPR), including requiring providing notice to government authorities. In addition, a news report dated March 20, 2019 reported that the Office of Personal Data Protection Malaysia's deputy commissioner, Rosmahyuddin Baharuddin, has also indicated that data breach notification is something that Malaysia is "seriously considering".

Notably, one of the issues for which feedback is sought in P01/2020 include reporting of data breaches. The points to be considered include, the proposed mandatory data breach notification, the impact of having all data users report about the data, and the elements to be considered in the guideline on data breach incident reporting.

ENFORCEMENT

Under the PDPA, the Commissioner is empowered to implement and enforce the personal data protection laws and to monitor and supervise compliance with the provisions of the PDPA. Under the Personal Data Protection Regulations 2013, the Commissioner has the

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 recently 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.'

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 is 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. Also, 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.

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

power to inspect the systems used in personal data processing and the data user is required, at all reasonable times, to make the systems available for inspection by the Commissioner or any inspection officer. The Commissioner or the inspection officers may require the production of the following during inspection:

- The record of the consent from a data subject maintained in respect of the processing of that data subject's personal data by the data user
- The record of required written notices issued by the data user to the data subject
- The list of personal data disclosures to third parties
- The security policy developed and implemented by the data user
- The record of compliance with data retention requirements
- The record of compliance with data integrity requirements, and
- Such other related information which the Commissioner or any inspection officer deems necessary

Violations of the PDPA and certain provisions of the Personal Data Protection Regulations 2013 are punishable with criminal liability. The prescribed penalties include fines, imprisonment or both. Directors, CEOs, managers or other similar officers will have joint and several liability for non-compliance by the body corporate, subject to a due diligence defense.

There is no express right under the PDPA allowing aggrieved data subjects to pursue a civil claim against data users for breaches of the PDPA.

However, under PCP 01/2020, the Commissioner has proposed to introduce a specific provision stating the right of a data subject to commence civil litigation against a data user.

ELECTRONIC MARKETING

The PDPA applies to electronic marketing activities that involve the processing of personal data for the purposes of commercial transactions. There are no specific provisions in the PDPA that deal with electronic marketing. However, the PDPA provides that a data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his or her personal data for direct marketing purposes. 'Direct marketing' means the communication by whatever means

industry sector in question. Civil penalties can be significant.

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.

As of January 1, 2020, California law (the CCPA) now 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.

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' (*eg*, 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

of any advertising or marketing material that is directed to particular individuals.

Pursuant to PCP 01/2020. the Commissioner is considering issuing a guideline to data users on the mechanism of digital and electronic marketing. The Commissioner has sought feedback on a proposed requirement on data users to provide a clear mechanism for data subjects to unsubscribe from online services and the elements to be considered in preparing the guideline on processing personal data in digital and electronic marketing.

The Commissioner is also considering issuing a guideline on the implementation of direct marketing for data users. Feedback from the public is sought as to whether a proposed data user is allowed to make the first direct marketing call to the data subject, the use of the 'opt-out' method, and the important elements to be considered in the preparation of such guideline.

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 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

ONLINE PRIVACY

There are no provisions in the PDPA that specifically address the issue of online privacy (including cookies and location data). However, any electronic processing of personal data in Malaysia will be subject to the PDPA and the Commissioner may issue further guidance on this issue in the future.

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 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; however, the law does not mandate

that companies provide consumers a 'Do-Not-Track' option. 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, given the CCPA's broad definition of personal information, information collected via cookies, online, mobile and targeted ads, and other online tracking are likely to be subject to the requirements of the law.

Further, given the CCPA's broad definition of personal information, information collected via cookies and similar technologies is generally subject to the requirements of the law (e.g., notice and consumer rights). In addition, 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. This broad definition may 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.

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. California law (the CCPA) also requires 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 *(eg,* mobile device) location information.

KEY CONTACTS

Skrine
www.skrine.com/

Jillian Chia
Partner
Skrine
T + 603 2081 3882
jc@skrine.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

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

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