DATA PROTECTION LAWS OF THE WORLD

United States vs Canada

DLA PIPER

UNITED STATES

Last modified 29 January 2023

LAW

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

Federal and State Privacy Laws and Regulations

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

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

CANADA

Last modified 26 January 2023

LAW

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, criminal code provisions etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The summary below focuses on Canada’s private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act ('PIPEDA')
- Personal Information Protection Act (Alberta) ('PIPA Alberta')
- Personal Information Protection Act (British Columbia) ('PIPA BC')
- Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Private Sector Act'), (collectively, 'Canadian Privacy Statutes')

On June 16, 2022, the federal Government introduced Bill C-27, a wide-reaching piece of legislation that is intended to modernize and strengthen privacy protection for Canadian consumers and provide clear rules for private-sector organizations. It is the second attempt to modernize federal private-sector privacy legislation, after a previous proposal died on the order paper in 2021. If adopted, Bill C-27 will replace PIPEDA with legislation specific to consumer privacy rights (the *Consumer Privacy Protection Act*) and electronic documents (the *Electronic Documents Act*). Bill C-27 will also introduce the *Artificial Intelligence and Data Act*, which aims to create rules around the deployment of AI technologies.

Key elements of Bill C-27 include:

- Clarified consent requirements for the collection, use and disclosure of personal information

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

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

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

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

- Expanded enforcement powers for the Office of the Privacy Commissioner of Canada, including stiff penalties for serious offenses of up ‎to 5% of annual gross global revenue or CA$25 million
- New rules governing de-identified information
- The creation of a specialized Personal Information and Data Protection Tribunal

C-27 is currently at the committee stage of the legislative process. There has been considerable debate over the Bill, in particular over the proposed *Artificial Intelligence and Data Act.* The final form of the language remains subject to material change.

PIPEDA applies to all of the following:

- Consumer and employee personal information practices of organizations that are deemed to be a ‘federal work, undertaking or business’ (*eg*, banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)
- Organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted ‘substantially similar’ legislation (PIPA BC, PIPA Alberta and the Quebec Private Sector Act have been deemed ‘substantially similar’)
- Inter provincial and international collection, use and disclosure of personal information in connection with commercial activity

PIPA BC, PIPA Alberta and the Quebec Private Sector Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

Quebec recently enacted a major reform of its privacy legislation with the adoption of Bill 64. Bill 64 received Royal Assent on September 22, 2021. A first set of amendments came into force on September 22, 2022, with additional modifications set to come into force on September 22, 2022, while the majority of substantial changes came into force on September 22, 2023. A third, more limited set of amendments will come into force on September 22, 2024. With Bill 64’s changes, Quebec now has in place a sophisticated legal framework for privacy and data protection that resembles the European GDPR in several key areas.

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

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

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

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

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

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

Enforcement of Unfair and Deceptive Trade Practices

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

their privacy and security practices.

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

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

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

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

DEFINITIONS

Definition of personal data

DEFINITIONS

Definition of personal data

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

California

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

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

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

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

Definition of sensitive personal data

Varies widely by sector and by type of statute.

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

‘Personal information’ includes any information about an identifiable individual (business contact information is expressly “carved out” of the definition of ‘personal information’ in some Canadian privacy statutes).

The Quebec Private Sector Act, as modified by Bill 64, has broadened the definition of “personal information” to include any information that allows an individual to be identified indirectly as well as directly. In Quebec, business contact information is included in the definition of “personal information”, however it is considered a less sensitive form of data to which many of the requirements of the Quebec Private Sector Act do not apply.

Definition of sensitive personal data

Not specifically defined in Canadian Privacy Statutes, except for the Quebec Private Sector Act.

The Quebec Private Sector Act, as modified by Bill 64, defines ‎‎“sensitive personal information” as any information ‎that, by virtue of its nature (e.g. biometric or medical), or because of the context in which it is used or communicated, warrants a high expectation of privacy. The Quebec Privacy Act has stricter consent requirements in certain situations for the use and communication of personal information qualified as sensitive.

Definition of anonymized information

The Quebec Private Sector Act, as modified by Bill 64, defines “anonymized information” as information concerning an individual which irreversibly no longer allows such individual to be identified, whether directly or indirectly. Quebec recently adopted a regulation which prescribes certain criteria and procedures which must be followed when anonymizing data.

Definition of de-identified information

The Quebec Private Sector Act, as modified by Bill 64, defines “de-identified information” as any information which no longer allows the concerned individual to be identified directly. “De-identified” information is still considered to be a form of personal information, to which most of the protections set out in the Quebec Private Sector Act continue to apply.

Definition of biometric information

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

The Quebec privacy regulator, the *Commission d’accès à l’information* (CAI), defines “biometric information” as information measured from a person’s unique physical, behavioural or biological characteristics. Biometric information is, by definition, sensitive information.

health status includes, but is not limited to:

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

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

NATIONAL DATA PROTECTION AUTHORITY

There is no single national authority.

With some exceptions (such as for banks, credit unions and insurance companies), the FTC has jurisdiction over most commercial entities and has authority to issue and enforce federal privacy regulations (including telemarketing, email marketing, and children's privacy) and

NATIONAL DATA PROTECTION AUTHORITY

Office of the Privacy Commissioner of Canada ('PIPEDA')‎

Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta')‎

Office of the Information and Privacy Commissioner for British Columbia ('PIPA ‎BC'), and

Commission d’accès à

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

l’information du Québec (the “CAI”) ('Quebec Private Sector Act')‎

REGISTRATION

There is no general registration requirement under Canadian Privacy Statutes.

Some registration requirements exist under Quebec

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.

privacy laws:

- Personal information agents, defined as “any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports”, must be registered with the CAI
- The use of certain biometric systems and the creation of databases of biometric information must be disclosed to and registered with the CAI

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.

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, and PIPA BC expressly require organizations to appoint an individual responsible for compliance with the obligations under the respective statutes.

The Quebec Private Sector Act, as modified by Bill 64, requires organizations to appoint a person responsible for the protection of personal information, who is in charge of ensuring compliance with privacy laws within the organization. By default, the person with the highest authority within the organization will be the person responsible for the protection of personal information, however this function can be delegated to any person, including a person outside of the organization.

This person’s responsibilities are broadly defined in the law and include:

- Approval of the organization’s privacy policy and ‎practices
- Mandatory privacy impact assessments
- Responding to and reporting security breaches, and
- Responding to and enacting access and ‎rectification rights

The contact information of the person responsible for the protection of personal information must be published online on the website of the organization.

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

COLLECTION & PROCESSING

Canadian Privacy Statutes set out the overriding obligation that organizations only ‎collect, use and disclose personal information for purposes that a reasonable person ‎would consider appropriate in the circumstances.‎

Subject to certain limited exceptions prescribed in the Acts, consent is required for the ‎collection, use and disclosure of personal information. Depending on the sensitivity of ‎the personal information, consent may need to be presented as opt-in or opt-out. Under the Quebec Private Sector Act, consent must be “clear, free and informed and be given for specific purposes”: this is generally interpreted as requiring opt-in consent in most situations, however depending on the context and sensitivity of the information, opt-out or implicit consent may, in certain specific situations, be considered valid. Organizations must limit ‎the

right to limit use of their sensitive data, and Iowa and Utah require individuals be provided a notice and right to opt-out of the collection of sensitive data.

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

collection of personal information to that which is necessary to fulfil the identified ‎purposes and only

    - the categories of third parties to whom the business discloses personal information and
    - the rights consumers have regarding their personal information and how to exercise those rights
- Include a “do-not-sell-or-share my information” link on the business's website and page where consumers can opt-out of the sale and sharing of their personal information (if applicable)
- Generally, provide at least two methods for consumers to submit CCPA requests to the 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

retain such personal information for as long as necessary to fulfil the ‎purposes for which it was collected.‎

Each of the Canadian Privacy Statutes have both notice and openness/transparency ‎requirements. With respect to notice, organizations are generally required to identify ‎the purposes for which personal information is collected at or before the time the ‎information is collected. With respect to openness/transparency, generally Canadian ‎Privacy Statutes require organizations make information about their personal ‎information practices readily available.‎

All Canadian Privacy Statutes contain obligations on organizations to ensure personal ‎information in their records is accurate and complete, particularly where the information ‎is used to make a decision about the individual to whom the information relates or if the ‎information is likely to be disclosed to another organization.‎

Each of the Canadian Privacy Statutes also provides individuals with the following:‎

- A right of access to personal information held by an organization, subject to limited ‎exceptions;
- A right to correct inaccuracies in/update their personal information records; and‎
- A right to withdraw consent to the use or communication of personal information.

In addition to these rights, the Quebec Private Sector Act, as modified by Bill 64, gives individuals the right to have their personal information deindexed. A right to data portability will be coming into force on September 22, 2024.

Finally, organizations must have policies and practices in place that give effect to the ‎requirements of the legislation and organizations must ensure that their employees are ‎made aware of and trained with respect to such policies.‎

denied, a method by which the consumer can submit a complaint to the state’s Attorney General.

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

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

TRANSFER

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

TRANSFER

When an organization transfers personal information to a third-party service provider (*ie*, ‎who acts on behalf of the transferring organization -- although Canadian legislation does not use these terms, the transferring organization would be the “controller” in GDPR parlance, and the service provider would be a “processor”), the transferring organization ‎remains accountable for the protection of that personal information and ensuring ‎compliance with the applicable legislation, using contractual or other means. In particular, the transferring organization is ‎responsible for ensuring (again, using contractual or other means) that the third party service provider appropriately safeguards ‎the data, and would also be required under the notice and openness/transparency ‎provisions to reference the use of third-party service providers in and outside of Canada ‎in their privacy policies and procedures.‎

These concepts apply whether the party receiving the personal information is inside or outside Canada. Transferring personal information outside of Canada for storage or processing is generally permitted so long as the requirements discussed above are addressed, and the transferring party notifies individuals that their information may be transferred outside of Canada and may be subject to access by foreign governments, courts, law enforcement or regulatory agencies. This notice is typically provided through the transferring party’s privacy policies.

With respect to the use of foreign service providers, PIPA Alberta specifically requires a ‎transferring organization to include the following information in its privacy policies and ‎procedures:‎

- The countries outside Canada in which the collection, use, disclosure or storage is ‎occurring or may occur, and
- The purposes for which the third party service provider outside Canada has been ‎authorized to collect, use or disclose personal information for or on behalf of the ‎organization

Under PIPA Alberta, specific notice must also be provided at the time of collection or ‎transfer of the personal information and must specify:‎

- The way in which the individual may obtain access to written information about the ‎organization’s policies and practices with respect to service providers outside ‎Canada, and
- The name or position name or title of a person who is able to answer on behalf of ‎the organization the individual’s questions about the collection, use, disclosure or ‎storage of personal information by service providers outside Canada for or on ‎behalf of the organization.‎

The Quebec Private Sector Act, as modified by Bill 64, requires all organizations to inform persons that their personal information may be transferred outside of Québec: this is typically done at the time the information is collected. Additionally, before transferring personal information outside of the province of Quebec, organizations conduct data privacy assessments and enact ‎appropriate ‎contractual safeguards to ensure that the information will benefit from adequate protection in the jurisdiction of transfer. These assessments must take into account the sensitivity of the information, the purposes, the level of protection (contractual or otherwise) and the applicable privacy regime of the jurisdiction of transfer. Cross-border transfers may only occur if the organization is satisfied that the information would receive an adequate level of protection. Quebec has decided not to implement a system of ‎adequacy decisions, and ‎therefore assessments are required prior to any ‎cross-jurisdiction transfer.

SECURITY

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

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organizations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information.

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

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

BREACH NOTIFICATION

Currently, PIPEDA, PIPA Alberta, and the Quebec Private Sector Act are the only Canadian Privacy Statutes ‎with breach notification requirements.‎

In Alberta, an organization having personal information under its control must, without ‎unreasonable delay, provide notice to the Commissioner of any incident involving the ‎loss of or unauthorized access to or disclosure of personal information where a ‎reasonable person would consider that there exists a real risk of significant harm to an ‎individual as a result.‎

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.

Notification to the Commissioner must be in writing and include:‎

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date or time period during which the loss or unauthorized access or disclosure ‎occurred
- A description of the personal information involved in the loss or unauthorized access ‎or disclosure
- An assessment of the risk of harm to individuals as a result of the loss or ‎unauthorized access or disclosure
- An estimate of the number of individuals to whom there is a real risk of significant ‎harm as a result of the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm to ‎individuals
- A description of any steps the organization has taken to notify individuals of the loss ‎or unauthorized access or disclosure, and
- The name and contact information for a person who can answer, on behalf of the ‎organization, the Commissioner’s questions about the loss of unauthorized ‎access or disclosure

Where an organization suffers a loss of or unauthorized access to or disclosure of ‎personal information as to which the organization is required to provide notice to the ‎Commissioner, the Commissioner may require the organization to notify the individuals ‎to whom there is a real risk of significant harm. This notification must be given directly ‎to the individual (unless specified otherwise by the Commissioner) and include:‎

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date on which or time period during which the loss or unauthorized access or ‎disclosure occurred
- A description of the personal information involved in the loss or unauthorized access ‎or disclosure
- A description of any steps the organization has taken to reduce the risk of harm, ‎and
- Contact information for a person who can answer, on behalf of the organization, ‎questions about the loss or unauthorized

access or disclosure

The breach notification provisions under PIPEDA are very similar to the breach ‎notification provisions under PIPA Alberta. The main difference is that PIPEDA requires organizations to notify both the affected individuals and the federal regulator if the breach creates a real risk of significant harm to the individuals (whereas PIPA Alberta requires the initial notice only to the regulator, and then to the individuals if the regulator requires it. In practice, many organizations notify affected Albertans regardless of whether the Alberta Commissioner requires (and the Commissioner typically does require it for most reported breaches in any event). Further, under PIPEDA, organizations must also ‎keep a record of ALL information security breaches, even those which do not meet the ‎risk threshold of a “real risk of significant harm.”‎

The Quebec Private Sector Act, as modified by Bill 64, introduced a number of new obligations in ‎connection with “confidentiality incidents”, which are defined as unauthorized access, use, or communication of personal ‎information, or the loss of such information, which were previously absent in Quebec privacy law‎. These include:‎

- A general obligation to ‎prevent, mitigate and remedy security incidents
- The obligation to notify the CAI and the person affected ‎whenever the incident presents a risk of ‎‎“serious ‎injury.” Factors to consider when evaluating the ‎risk of serious injury include the sensitivity of the ‎information ‎concerned, the anticipated consequences of the ‎use of the information and the likelihood ‎that the information will ‎be used for harmful purposes. Although the Quebec Private Sector Act requires organizations to act “promptly” and “with diligence” in response to confidentiality breaches, it does not provide specific timeframes within which such notifications must be made, and
- The obligation on to keep a register of confidentiality ‎incidents, with the CAI having extensive audit rights

Quebec recently adopted regulations further detailing the reporting, notification, and record-keeping obligations of organizations in connection with confidentiality incidents.

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 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).

ENFORCEMENT

Canadian privacy regulatory authorities have an obligation to investigate complaints, as well as the authority to initiate complaints.

Under PIPEDA, a complaint must be investigated by the Commissioner and a report will be prepared that includes the Commissioner’s findings and recommendations. A complainant (but not the organization subject to the complaint) may apply to the Federal Court for a review of the findings and the court has authority to, among other things, order an organization to correct its practices and award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organizations are required to comply with the order within a prescribed time period, or apply for judicial review. In both BC and Alberta, once an order is final, an affected individual has a cause of action against the organization for damages for loss or injury that the individual has suffered as a result of the breach.

In Alberta and BC, a person that commits an offence may be subject to a fine of not more than CA$100,000. Offences include, among other things, collecting, using and disclosing personal information in contravention of the Act (in Alberta only), disposing of personal information to evade an access request, obstructing the commissioner, and failing to comply with an order.

Similarly, under the Quebec Private Sector Act, an order from the CAI must be complied with within a prescribed time period. An individual may appeal to the judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.

The Quebec Private Sector Act, as modified by Bill 64, introduced a regime of steep fines and administrative penalties in case of non-compliance. The maximum penalties range between CA$5,000 and CA$100,000 in the case of individuals, and up to between CA$15,000$ and CA$25 million or 4% of worldwide turnover for the preceding fiscal year for organizations. This new penalty regime represents a significant change with the previous Quebec regime, under which the maximum penalties were limited to CA $20,000.

There are also statutory privacy torts in various provinces under separate legislation, and Ontario courts have recognized a common-law cause of action for certain

ELECTRONIC MARKETING

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

Email

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

Text Messages

Federal and state regulations apply to the sending of marketing text messages to individuals. Express consent is 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 privacy torts. In Quebec, a general right to privacy also exists under the *Civil Code of Quebec* and the *Charter of Human Rights and Freedoms*. Organizations may face litigation (including class action litigation) under these statutory and common-law torts, as well as under the general regime of civil liability in Quebec, in addition to any enforcement or claims under Canadian Privacy Statutes.

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed ‎above), as well as Canada’s Anti-Spam Legislation (CASL).‎

CASL is a federal statute which prohibits sending, or causing or permitting to be sent, a commercial electronic message (defined broadly to include text, sound, voice, or image messages aimed at encouraging participation in a commercial activity) unless the recipient has provided express or implied consent and the message complies with the prescribed content and unsubscribe requirements (subject to limited exceptions).

What constitutes both permissible express and implied consent is defined in CASL and its regulations. For example, an organization may be able to rely on implied consent when there is an “existing business relationship” with the recipient of the message, based on:

- A purchase by the recipient within the past two years, or
- A contract between the organization and the recipient currently in existence or which ‎expired within the past two years

CASL also prohibits the installation of a computer program on any other person's ‎computer system, or having installed such a computer program to cause any electronic ‎messages to be sent from that computer system, without express consent, if the ‎relevant system or sender is located in Canada. In addition, the Act contains anti ‎phishing provisions that prohibit (without express consent) the alteration of transmission ‎data in an electronic message such that the message is delivered to a destination other ‎than (or in addition to) that specified by the sender.‎

CASL also introduced amendments to PIPEDA that restrict 'address harvesting', or the ‎unauthorized collection of email addresses through automated means

consent. This is a significant class action risk area, and any campaign or program that involves calls (marketing or informational) to phone numbers that may be wireless phone numbers needs to be carefully reviewed for strict compliance with legal requirements. The definition of autodialing equipment is generally considered to, broadly, include any telephone system that is capable of (whether or not used or configured storing or producing telephone numbers to be called, using a random or sequential number generator.

Telemarketing

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

Fax Marketing

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

(i.e., using a ‎computer program designed to generate or search for, and collect, email addresses)

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 ‎without consent. The use of an individual’s email address collected through address ‎harvesting also is restricted.‎

The 'Competition Act' was also amended to make it an offence to provide false or ‎misleading representations in the sender information, subject matter information, or ‎content of an electronic message.‎

CASL contains potentially stiff penalties, including administrative penalties of up to ‎CA$1 million per violation for individuals and CA$10 million for corporations (subject to a ‎due diligence defense). CASL also sets forth a private right of action permitting ‎individuals to bring a civil action for alleged violations of CASL (CA$200 for each ‎contravention up to a maximum of CA$1 million each day for a violation of the ‎provisions addressing unsolicited electronic messages). However, the private right of ‎action is not yet in force, and there is currently little expectation that it will ever come into force.‎

ONLINE PRIVACY

Online privacy is governed by Canadian Privacy Statutes (discussed above). In ‎general, Canadian privacy regulatory authorities have been active in addressing online ‎privacy concerns.‎

For example, in the context of social media, the OPC has released numerous Reports ‎of Findings addressing issues including:‎

- Default privacy settings
- Social plug-ins
- Identity authentication practices, including data scraping and voiceprint
- The collection, use and disclosure of personal information on social networking sites, including for marketing purposes‎
- The OPC has also released decisions and guidance on privacy in the context of ‎Mobile Apps

In addition, the OPC has released findings and guidelines related to the use of cookies ‎and online behavioral advertising, including findings indicating that information stored by ‎temporary and persistent cookies is considered to be personal information and ‎therefore subject to PIPEDA. The OPC has

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

adopted the same position with respect to ‎information collected in connection with online behavioral advertising.‎

In ‘Privacy and Online Behavioral Advertising’, the OPC stated that it may be permissible to use opt-out consent in the context of online behavioral advertising if the following conditions are met:‎

- Individuals are made aware of the purposes for the online behavioral advertising, at ‎or before the time of collection, in a manner that is clear and understandable
- Individuals are informed of the various parties involved in the online behavioral ‎advertising at or before the time of collection
- Individuals are able to opt-out of the practice and the opt-out takes effect ‎immediately and is persistent
- The information collected is non-sensitive in nature (*ie*, not health or financial ‎information), and
- The information is destroyed or made de-identifiable as soon as possible

The OPC has indicated that online behavioral advertising must not be a condition of ‎service and, as a best practice, should not be used on websites directed at children.‎

Canadian privacy regulatory authorities also consider location data, whether tied to a static location or a mobile device, to be personal information. As such, any collection, use or disclosure of location data requires, among other things, appropriate notice, and consent. Most of the privacy regulatory authority decisions related to location data have arisen with respect to the use of GPS in the employment context.

The Canadian privacy regulatory authorities provide the following test that must be met ‎for the collection of GPS data (and other types of monitoring and surveillance activities):‎

- Is the data demonstrably necessary to meet a specific need?‎
- Will the data likely be effective in meeting that need?‎
- Is the loss of privacy proportional to the benefit gained? ‎
- Are there less privacy-intrusive alternatives to achieve the same objective?‎

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.

Bill 64 introduced several changes to the Quebec Private Sector Act which significantly impact online privacy. Starting September 22, 2023, organizations collecting personal information by offering a product or service with privacy parameters must ensure that the highest privacy settings are enabled by default. Additionally, organizations collecting personal information from persons using tracking, localization or profiling technology (including cookies, trackers, and similar technologies) have the obligation to inform the person in advance of the use of such technologies, and to inform the person of the method for activating such functions: the use of such technologies therefore requires opt-in consent. “Profiling” is broadly defined as the collection and use of personal information in order to evaluate certain characteristics of a person such as workplace performance, economic or financial situation, health, personal preferences or interest, or behaviour.

Artificial Intelligence

The OPC has also issued guidance on the appropriate use of generative AI systems and has stated that generative AI systems should be developed with the general principles of legality, appropriate purposes, necessity and proportionality, openness and accountability, and:

- In a manner that allows individuals to meaningfully exercise their rights to access their personal information; while
- limiting collection, use and disclosure to only what is needed to fulfill the identified purpose; and
- implementing appropriate safeguards

In addition, the OPC has stated that developers of generative AI models should take steps to ensure that outputs should be as accurate as possible.

KEY CONTACTS

Tamara Nielsen
Counsel
T +1 604.643.2952
tamara.nielsen@dlapiper.com

DATA PRIVACY TOOL

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

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.

protection maturity.