Data Protection & Privacy 2021

Contributing editors
Aaron P Simpson and Lisa J Sotto

LEXOLOGY
Getting The Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development manager
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Ninth edition
ISBN 978-1-83862-322-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Data Protection & Privacy

2021

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting The Deal Through is delighted to publish the ninth edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting The Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting The Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Canada and Romania.

Lexology Getting The Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting The Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY®
Getting The Deal Through

London
August 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2020
For further information please contact editorial@gettingthedealthrough.com

Contents

Canada

Doug Tait and Catherine Hamilton*
Thompson Dorfman Sweatman LLP

LAW AND THE REGULATORY AUTHORITY

Legislative framework

1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

In Canada, four private sector privacy enactments provide the framework for the protection of PII. These are:

- Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA);
- the province of Québec's An Act Respecting the Protection of Personal Information in the Private Sector (Private Sector Act (QC));
- the province of Alberta's Personal Information Protection Act (PIPA (AB)); and
- the province of British Columbia's Personal Information Protection Act (PIPA (BC)).

PIPEDA governs the interprovincial and international collection, use or disclosure of PII by private sector organisations in the course of carrying out commercial activities for profit. It also has application to employee PII in federally regulated organisations (such as banks, airlines, railways, and telecommunication companies).

PIPEDA also applies within all provinces and territories in Canada, except Québec, Alberta and British Columbia. The Private Sector Act (QC), PIPA (AB) and PIPA (BC) have been deemed substantially similar to PIPEDA and as such PIPEDA does not apply to private sector organisations carrying out commercial activities wholly within those provinces.

While the Private Sector Act (QC), PIPA (AB) and PIPA (BC) have each been deemed substantially similar to PIPEDA, there are differences in the details of each. These provincial laws apply, generally speaking, to all private sector organisations with respect to the collection, use and disclosure of PII in the course of carrying out commercial activities and to employees' PII. The Private Sector Act (QC) also applies to the private sector's collection, use and disclosure of health PII.

Health information privacy legislation in the provinces of Ontario, New Brunswick, Nova Scotia and Newfoundland, and Labrador have been deemed substantially similar to PIPEDA and apply to health PII within those provinces. In those provinces and territories where health information privacy legislation has not been deemed substantially similar to PIPEDA, both the provincial or territorial health information privacy legislation and PIPEDA may apply.

Privacy matters involving public sector institutions are governed by a variety of federal, provincial and territorial public sector privacy legislative enactments.

Certain provinces have enacted legislation recognising invasion of privacy as statutory tort, while there are also various offenses within the Criminal Code (Canada) regarding the invasion of privacy.

Data protection authority

2 Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no single regulatory authority dedicated to overseeing and enforcing data protection laws in Canada. The applicable regulatory authority varies based upon whether the matter is appropriately covered by federal or provincial privacy laws.

While the Office of the Privacy Commissioner of Canada (OPC) oversees and enforces PIPEDA, each province and territory of Canada has a commissioner or ombudsperson responsible for overseeing and enforcing its own provincial or territorial privacy legislation. In the case of Québec, Alberta and British Columbia their privacy legislation is overseen and enforced by the *Commission d'accès à l'information du Québec* (CAI), the Office of the Information & Privacy Commissioner of Alberta and the Office of the Information & Privacy Commissioner for British Columbia, respectively.

Under PIPEDA, the OPC has the power to investigate complaints made by individuals. The OPC can also initiate an investigation based on reasonable grounds to believe that a matter warrants it. Under its investigatory power, the OPC has the power to summon witnesses to give oral or written evidence, inspect documents and compel the production thereof, and inspect premises other than a dwelling house. The OPC, upon having reasonable grounds to believe that an organisation is contravening PIPEDA, has the authority to audit the organisation's PII practices, including examining the policies, procedures and practices of an organisation, exploring the physical and security controls of an organisation, and inspecting an organisation's incident response management protocols.

The CAI, under Québec's An Act Respecting the Protection of Personal Information in the Private Sector, and the Commissioners, under Alberta's Personal Information Protection Act and British Columbia's Personal Information Protection Act, each have similar investigatory powers, and where necessary, the power to conduct an inquiry. Following an inquiry, each also has the power to issue orders.

Cooperation with other data protection authorities

3 Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There are no legal obligations on Canadian data protection authorities to cooperate with other data protection authorities. However, the OPC has the express authority under PIPEDA to share information with provincial

and territorial counterparts in the context of an ongoing or potential investigation of a complaint or audit. Canadian privacy commissioners and ombudspersons may also develop and publish joint publications or guidelines related to the protection of PII. The OPC may also share information with a foreign data protection counterpart pursuant to a written information sharing arrangement.

Breaches of data protection

4 | Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

In Canada, breaches of federal and provincial privacy laws can result in sanctions or orders, or criminal penalties.

Under PIPEDA, certain breaches can, if an organisation is found guilty, result in monetary fines. However, as it currently stands, the OPC does not have the authority under PIPEDA to prosecute offences or issue fines. As such, where it believes an offence has been committed, the matter must be referred to the office of the Attorney General of Canada, who, after its investigation, determines potential prosecution.

SCOPE

Exempt sectors and institutions

5 | Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) does not cover any private sector, for profit, commercial organisation operating wholly within the provinces of Québec, Alberta and British Columbia, nor does it cover employee personally identifiable information (PII) of private sector, for profit, commercial organisations that are not federally regulated. It also does not cover organisations that are not engaged in for profit commercial activities (such as, generally speaking, not-for-profits, charities and political parties).

Organisations that collect PII solely for 'journalistic, artistic or literary purposes' are also exempt from PIPEDA.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Electronic marketing is regulated by the Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act and its regulations (as amended). This legislation is commonly known as 'Canada's Anti-Spam Legislation' (CASL).

PIPEDA will apply to the same activities where the processing of PII is involved.

Private sector privacy laws generally permit overt or covert video surveillance and the recoding of phone calls, but both must be balanced with an individual's right to privacy and to achieve a specific purpose. As a general rule, organisations should consider less intrusive means of achieving the same end before conducting video surveillance. In addition, certain provinces have enacted statutory privacy torts for violation of privacy in which surveillance or the listening to, or recording of, a conversation may be a violation of an individual's privacy.

The Criminal Code sets out privacy-related offences, specifically the interception of communications and provisions governing how law enforcement may obtain judicial authorisation to conduct electronic surveillance for criminal investigations.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

There are numerous federal and provincial laws that provide for specific privacy and data protection rules and laws that apply to, among other things, banking, credit unions, financial transactions, electronic commerce, consumer credit reporting, health and health records or data which contains specific confidentiality provisions concerning PII that is collected.

PII formats

8 | What forms of PII are covered by the law?

The basic concept in Canadian privacy law is that PII is any information, recorded or not, about an identifiable individual, regardless of what format it may be held. Examples of PII are:

- age, name, assigned identification numbers, income, ethnic origin, religion, marital status, fingerprints or blood type;
- opinions, evaluations, comments, social status or disciplinary actions;
- education, medical, criminal and employment histories;
- information about financial transactions; and
- employee files, credit records, loan records and medical records.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

PIPEDA is silent as to its territorial scope. However, the Federal Court of Canada has held that, in the absence of language clearly limiting its application to Canada, PIPEDA can be interpreted to apply in all circumstances in which there exists a 'real and substantial link' between an organisation's activities and Canada.

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

Under PIPEDA, the organisation that determines the purpose of collection and collects, uses and discloses the PII is in control of that information. The same organisation may also process the PII itself or transfer it to a third party (either within or outside of Canada) for processing. Even though PII may be transferred to a third party for processing, it is the controlling organisation that remains in control of, and is ultimately responsible for, the PII.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

11 | Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

In general, subject to limited exceptions, Canadian privacy legislation requires organisations to obtain meaningful consent for the collection, use and disclosure of personally identifiable information (PII). What

constitutes 'meaningful consent' is guided by seven principles designed to ensure that the individual providing the consent has, among other things, a clear understanding of the nature, purpose and consequence of what they are consenting to, been provided information, in a clear and comprehensible manner, about the organisation's privacy management practices, and been provided with a clear 'yes' or 'no' option.

An organisation cannot not require consent as a condition for providing a product or service, beyond that required to fulfil an explicitly specified and legitimate purpose. The form of consent, whether express or implied, may vary depending on the nature of the PII and the reasonable expectations of the individual. Individuals may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

Privacy legislation generally states that the more sensitive the PII, the greater the security safeguards required to protect it. Legislation does not always specifically state what types of security safeguards ought to be implemented, but rather leaves it to an organisation to determine what is appropriate in the circumstances. In addition, the vast majority of provinces have health legislation that applies specifically to entities that fit within the definition of 'custodians' or 'trustees' and have stricter and more specific standards of security safeguards for health PII.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Canadian privacy law is based on consent. As such, the obtaining of meaningful consent, either express or implied, is necessary for an organisation's collection, use and disclosure of PII. Accordingly, apart from mandatory breach notifications in the event of a breach of security safeguards that could reasonably create a real risk of significant harm to an individual; or notifications that may be required pursuant to a proposed transfer of personally identifiable information (PII) outside of its jurisdiction, or a request to access information from an affected individual, there is no law of general application that requires organisations to notify individuals whose PII they hold.

In the case of mandatory breach notifications, the notification must be conspicuous and include enough information to allow the individual to understand the significance of the breach to them and to take steps, if possible, to reduce or mitigate the risk of harm.

Exemption from notification

14 | When is notice not required?

Apart from mandatory breach notifications in the event of a breach of security safeguards that could reasonably create a real risk of significant harm to an individual; or notifications that may be required pursuant to a proposed transfer of PII outside of its jurisdiction, or a request to access information from an affected individual, there is no law of general application that requires organisations to notify individuals whose PII they hold.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Generally, individuals have the right to acquire information as to an organisation's PII handling practices and policies without unreasonable effort. Individuals also have the right:

- to gain access to their PII;
- to know whether and what type of PII is held;
- a general account of the use and disclosure of their PII; and
- the right to amend PII if it is inaccurate or incomplete.

Data accuracy

16 | Does the law impose standards in relation to the quality, currency and accuracy of PII?

Canadian privacy legislation contains obligations for organisations to ensure that the PII that it uses, collects and discloses is accurate, complete and up to date, particularly where the information is used to make a decision about the individual to whom the information relates or is likely to be disclosed to another organisation.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

Canadian private sector privacy legislation provides that the amount of PII that an organisation holds should be limited to what is necessary for the identified purpose. Canadian privacy legislation also provides that, absent any specific legislative requirements to keep the PII for a certain period of time, the PII should be held only as long as is necessary to fulfil its identified purpose and once it is no longer required to fulfil such purpose it should be destroyed, erased or made anonymous.

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Organisations are generally required to identify the purposes for which PII is collected at or before the time the information is collected. Organisations shall also document such purposes in order to be transparent about privacy practices. PII must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as permitted or required by law.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

If an organisation wishes to use PII in its possession for a new purpose, it must obtain consent from individuals to use their PII for the newly identified purpose.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Canadian privacy legislation requires that organisations implement reasonable technical, physical and administrative safeguards

to adequately protect personally identifiable information (PII) against loss or theft and from unauthorised access, disclosure, copying, use or modification, regardless of the format in which it is held. Specific security safeguards are generally not included in legislation and the onus is placed on the organisation to ensure that, through the use of appropriate security safeguards, the PII is adequately protected.

In assessing what constitutes 'appropriate security safeguards', consideration must be given to the nature of the PII and the harm that might result from its loss, theft unauthorized access, disclosure, copying, use or modification. As the sensitivity of the PII increases, so increases the assumed risk of harm, thereby increasing what constitutes an appropriate level of security safeguards.

Where organisations engage service providers to process PII on their behalf, such organisations remain responsible for protecting the PII. They have an obligation to ensure, through contractual or other means, that the service providers are themselves using appropriate security safeguards to provide an adequate level of protection for the PII in their possession.

Certain types of PII, such as that related to health or financial matters, may also be subject to industry specific legislation that imposes specific security obligations on the owners of PII.

Notification of data breach

21 | Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Currently, Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) and Alberta's Personal Information Protection Act (PIPA (AB)) are the only jurisdictions containing mandatory breach notification requirements. Under PIPEDA, an organisation that suffers a breach of security safeguards involving PII under its control and that poses a real risk of significant harm to individuals, must:

- report to the Office of the Privacy Commissioner of Canada (OPC);
- notify affected individuals as soon as feasible; and
- notify any government institution or organisation that it believes can reduce or mitigate the risk of harm that could result from the breach.

The report to the OPC must be made in prescribed form and the notice to the affected individuals must contain the information set out in the regulations.

Organisations under PIPEDA are also required to keep records, in prescribed form, of all breaches of security safeguards involving PII under its control, and to provide the Privacy Commissioner with a copy of such records on request. Those records must be kept for at least two years.

The breach notification provisions under PIPA (AB) are very similar to those under PIPEDA. However, there is no obligation to keep a record of all security breaches.

INTERNAL CONTROLS

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta's Personal Information Protection Act and British Columbia's Personal Information Protection Act expressly require organisations to appoint an individual who is accountable for ensuring compliance with the organisation's data protection obligations and who may, in turn, delegate some of his or her responsibilities to others. Such individuals are typically referred to as the 'chief privacy officer' or 'privacy officer', though the legislation does not prescribe any particular title. They are generally accountable for an organisation's policies and practices and is the designated individual to respond to inquiries, complaints, and access requests. Currently, there is no similar requirement under Québec's An Act Respecting the Protection of Personal Information in the Private Sector.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

Absent a breach of security safeguards, there is no specific record-keeping requirement for private sector organisations, subject to any industry specific requirements. In addition, certain provincial health-related legislation requires maintaining records in certain circumstances.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

Within the context of the private sector, there are no legal obligations in relation to new processing operations, such as to apply a privacy-by-design approach or carry out privacy impact assessments. However, in the context of the public sector, certain of the provincial or territorial privacy enactments require, in certain circumstances, that privacy impact assessments be performed in the context of the design and development of products and services.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

As a rule, organisations that collect, use or disclose personally identifiable information (PII) do not have a legal obligation to register with a supervisory authority. Organisations that wish to use or disclose PII, without consent, for statistical or scholarly study or research purposes must however notify the Office of the Privacy Commissioner of Canada before such use or disclosure.

Formalities

26 | What are the formalities for registration?

No registration with a supervisory authority is required.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

There is no register.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

There is no register.

Public access

29 | Is the register publicly available? How can it be accessed?

There is no register.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

There is no register.

Other transparency duties

31 | Are there any other public transparency duties?

Canadian privacy legislation, generally speaking, requires organisations to establish policies and practices detailing how the organisation addresses privacy and related obligations under the various pieces of legislation. While, for the most part, the legislation leaves the exact nature of the policies and practices to the discretion of the organisation, it is now accepted that, at the very least, an organisation must have a public-facing privacy policy.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Organisations are responsible for the personally identifiable information (PII) they collect, use and disclose, even when it is being transferred to a third party. As such, while organisations are, in general, permitted to transfer PII to third parties, without consent, they must ensure, through contractual or other means, that a comparable level of protection is afforded to the PII when the PII is processed by a third party. Moreover, the PII can only be used by a third party for the purposes for which it was originally collected and organisations must be transparent about their information-handling practices.

Restrictions on disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

The disclosure of PII to other recipients generally requires the consent of affected individuals. However, there are exceptions to the consent requirement when disclosing PII to comply with the rules of court relating to the production of records, and where required or permitted by law. When disclosing PII in either context, the remaining requirements of the applicable privacy legislation still apply and organisations must only disclose the PII in the manner and to the extent to which a reasonable person would consider appropriate in the circumstances, must limit the amount of PII that is disclosed to that which is reasonably necessary in the circumstances, and must appropriately safeguard the transmission of the PII.

Cross-border transfer

34 | Is the transfer of PII outside the jurisdiction restricted?

Neither Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) nor any other private sector provincial privacy legislation expressly prohibit the transfer of PII outside of Canada. However, organisations are required to use contractual or other means to provide the PII with a comparable level of protection to that which it would have received in Canada while the PII is outside the jurisdiction. Moreover, the transfer of the PII must only be used for the purposes for which the PII was initially collected and organisations must be transparent about their information handling practices, including notifying individuals whose PII is being processed that, among other things, their data is being sent elsewhere.

Alberta's Personal Information Protection Act (PIPA (AB)) contains statutory requirements for the transfer of PII outside of Canada. Under PIPA (AB) an organisation intending to transfer PII outside of Canada for processing must first provide notice to individuals of its policy and procedures addressing such transfers, and contact information of its representative who can respond to questions regarding such activities. The organisation should also notify the individuals concerned that transfers of data may be made.

The Québec's An Act Respecting the Protection of Personal Information in the Private Sector (Private Sector Act (QC)) limits the transfer of PII outside of Québec to jurisdictions that have privacy protection legislation in place equivalent to that which exists in Québec.

Alberta and Québec restrict the transfer of public sector PII outside of Canada and, in some instances outside these respective provinces. With limited exceptions, consent of the affected individuals being one, British Columbia and Nova Scotia prohibit government institutions and Crown agents, as well as their service providers, from transferring PII outside of Canada. Nova Scotia and Newfoundland and Labrador restrict the transfer of health PII outside each respective province.

In addition, the Private Sector Act (QC) requires public sector organisations to consider the potential risks involved in transferring PII outside of Québec. If the information will not receive adequate protection, it must not be transferred.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Cross-border transfers of PII do not require a notification to or the authorisation of a supervisory authority.

Further transfer

36 | If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

To the extent that transfers outside of Canada are subject to obligations, such obligations apply equally to transfer to service providers and onward transfers.

RIGHTS OF INDIVIDUALS

Access

37 | Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Under Canadian privacy legislation, organisations must, upon request and subject to limited exemptions, inform individuals of the existence, use and disclosure of an individual's personally identifiable information (PII), and must give them access to that information, including a listing of the third-party organisations with whom the information has been shared.

The right of "access" does not oblige an organisation to provide copies of PII records; rather, it requires the provision of access, which may include viewing the records at an organisation's offices. Generally, an individual's request must be sufficiently specific as to allow an organisation to identify the records.

Under Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) and British Columbia's Personal Information Protection Act (PIPA (BC)), an organisation must respond to an access request no later than 30 days after receipt of the request. Under Alberta's Personal Information Protection Act (PIPA (AB)), an organisation must respond to an access request not later than 45 days after receipt of the request. Each of the Acts contains provisions enabling an organisation, in certain circumstances, to extend the prescribed time frame for a response by another 30 days. While the circumstances vary slightly depending on the legislation, one common example is where additional time is required to undertake consultations with another organisation prior to responding to the request.

Under Québec's An Act Respecting the Protection of Personal Information in the Private Sector (Private Sector Act (QC)), an organisation must respond to an access request no later than 30 days after the date of the receipt of the request. Failure to respond within this time frame is deemed to be a refusal to grant the request.

Under PIPEDA, PIPA (BC) and PIPA (AB) access must be granted at minimal or no cost to the individual, and must make the information available in a form that is generally understandable.

Under the Private Sector Act (QC) access must be provided free of charge. However, a reasonable charge may be required from a person requesting a transcription, reproduction or transmission of the PII in question.

The exemptions to the right of access vary amongst legislation and need to be carefully considered. Examples of the statutory exemptions include, but are not limited to, information subject to solicitor-client or litigation privilege, confidential commercial information, information about another individual, information that relates to national security matters, and information generated in a formal dispute resolution process.

Other rights

38 | Do individuals have other substantive rights?

Generally, individuals have the following rights in relation to PII held by organisations:

- to gain access to PII, including whether and what type of PII is held and a general account of its use and disclosure;
- to amend PII if it is inaccurate or incomplete;
- to acquire information as to an organisations' PII handling practices and policies without unreasonable effort, including that PII is made available to related organisations, such as subsidiaries;
- to withdraw consent at any time, subject to any contractual or legal restrictions, reasonable notice. The individual must be informed of the implications of withdrawal of consent; and
- to make a complaint to the relevant privacy authority. Prior to doing so, individuals should address privacy issues with the designated Privacy Officer or equivalent within the organisation who is accountable for the organisation's compliance.

Whether there is a General Data Protection Regulation (GDPR) type 'right of erasure' of PII is currently unsettled in Canada.

Compensation

39 | Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals affected by breaches of the law and seeking monetary damages or compensation must seek redress through private legal action. Such individuals may be entitled to monetary damages or compensation for wrongful acts either under the common law or pursuant to those statutes that provide for a private right of action. As a general rule, individuals must establish that they suffered actual damages as a direct result of negligent actions in order to be successful.

Enforcement

40 | Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of individuals affected by breaches of the law and seeking monetary damages or compensation is exercisable primarily through the judicial system. Typically, the civil penalties imposed by supervisory authorities are not paid directly to aggrieved individuals, but there are exceptions.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Under Canadian privacy legislation, there are both mandatory and discretionary exceptions to the consent, use and disclosure of PII. The type of exceptions will depend upon the PII at issue, jurisdiction, and whether an organisation is in the public or private sector. The specific applicable legislation ought to be consulted to carefully determine if any applicable exceptions exist. Some common types of exceptions centre around PII related to an investigation, national security, artistic or literary purposes, study of research purposes, or protecting the health or safety of individuals.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

As the enforcement powers of supervisory authorities in Canada are very limited, organisations collecting, using and disclosing PII do not so much have a right of appeal against orders of a supervisory authority, but rather a right to apply for a hearing before the courts. Under Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA), after receiving a report from the Office of the Privacy Commissioner of Canada (OPC), which is non-binding, or being notified that the investigation of a complaint has been discontinued, a complainant may, subject to certain limitations, apply to the Federal Court of Canada for a de novo hearing regarding any matter in respect of which the complaint was made or that is referred to in the OPC report. The court has broad remedial powers, including the ability to order the imposition of fines for noncompliance with certain provisions of PIPEDA, correct an organisation's practices or award damages to the complainant.

In Alberta and British Columbia, organisations have the right, exercisable within a prescribed time, to apply for a judicial review or orders made under Alberta's Personal Information Protection Act or British Columbia's Personal Information Protection Act. In Québec, an individual may appeal orders made under Quebec's An Act Respecting the Protection of Personal Information in the Private Sector to a judge of the Court of Québec on questions of law or jurisdiction with respect to a final decision.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe any rules on the use of 'cookies' or equivalent technology.

Canada does not have specific legislation regulating 'cookies'. Rather, 'cookies', are subject to Canada's Anti-Spam Legislation (CASL) and privacy laws. Under CASL, express consent must be obtained prior to installing any kind of computer program on another's computer in the course of commercial activity. To obtain express consent the purpose for which consent is sought, the identity of the person seeking consent must be identified. CASL also states that a person's conduct can be an indication of express consent to the installation of 'cookies' if it is reasonable to believe that the person has consented through their actions.

Under privacy laws, consent may be obtained through express or implied. To the extent that the PII is sensitive in nature, express consent is required. If the PII is non-sensitive in nature, implied (or opt-out) consent is acceptable online behavioural advertising, provided that:

- individuals are made aware of the purposes for the practice in a manner that is clear and understandable;
- individuals are informed of the purposes at or before the time of collection, and are provided with information about the various parties involved in online behavioural advertising;
- individuals are able to easily opt out of the practice at or before the time the information is collected;
- the opt-out takes effect immediately and is persistent;
- the information collected and used is limited, to the extent practicable, to non-sensitive information; and
- information collected and used is destroyed or effectively anonymised as soon as possible.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

Unless an exception or exemption applies, it is unlawful under CASL to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include text, sound, voice or image messages) to an electronic address, unless the recipient has provided express or implied consent and the message complies with the prescribed form and content requirements, including containing an unsubscribe mechanism.

CASL also prohibits the installation of software on a person's computer without the consent of the device's owner. A person is considered to have consented to the software installation if their conduct is such that it is reasonable to believe they consented to the software installation. CASL does not apply to a person or business who installs software on their own computer, for example, or to updates, patches or bug fixes.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

There are no specific rules or legislation that governs the processing of PII through cloud computing services. However, the OPC, in conjunction with the Offices of the Information and Privacy Commissioner of Alberta and British Columbia, has developed guidance documentation to provide organisations with general information on cloud computing, to help them understand the privacy implications and responsibilities associated with PII being handled by a cloud provider, and to offer some suggestions to address privacy considerations in the cloud.

THOMPSON DORFMAN SWEATMAN

B Douglas Tait
bdt@tdslaw.com

Catherine M Hamilton
cmh@tdslaw.com

Suite 1700
242 Hargrave Street
Winnipeg
Manitoba
Canada R3C 0V1
Tel: +1 204 957 1930
www.tdslaw.com

UPDATE AND TRENDS

Key developments of the past year

46 | Are there any emerging trends or hot topics in international data protection in your jurisdiction?

There is a widely held belief that Canada's privacy laws are in need of reform. In 2019, the government of Canada released a Digital Charter Action Plan proposing to reform and modernise Canada's federal Personal Information Protection and Electronic Documents Act. The Digital Charter set out 10 principles that the government intends to use as the foundation for its reforms, including giving Canadians more control over their data and enhancing enforcement powers. As of this date, there has been no legislation passed to implement any changes.

The government of Canadian also currently studying reforms to the Privacy Act.

In British Columbia, a special committee has been appointed to review British Columbia's Personal Information Protection Act and to submit a report of its findings to the provincial government.

In Québec, the provincial government recently announced plans to modernise Quebec's Act Respecting the Protection of Personal Information in the Private Sector. It is expected that these reforms will model privacy standards similar to those found in the European Union's General Data Protection Regulation.

* *The writers would like to acknowledge Bryan A Tait - articling student, for his contributions to the preparation of this chapter.*

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

ISBN 978-1-83862-322-7