fogler rubinoff

David Young Law
Privacy and Regulatory Law Counsel

Council of Canadian Innovators[1] CEO Briefing on Bill C-27

How Canada's proposed private sector modernized privacy law and new AI systems law will impact Canadian businesses

by
Bill Hearn, Partner, Fogler Rubinoff LLP
and
David Young, Principal, David Young Law

July 12, 2022*
*Updated August 3, 2022

Outline

- Background to and summary of Bill C-27
- Accountability and privacy management programs
- Reinforced conditions for valid consent
- Certain "business activities" and "legitimate interest" exceptions to consent
- Obligations of service providers
- Cross-border transfers of personal information
- Codes of practice and certification programs
- De-identification and anonymization
- Individual rights to data mobility, disposal, explanation in automated decision systems
- Increased risks for non-compliance – new model, powers, tools, administrative monetary penalties, fines, private right of action
- Oversight of high-impact AI systems – the new *Artificial Intelligence and Data Act*
- Comparisons to privacy laws in Europe
- Key differences from old Bill C-11
- Key takeaways for Canadian business
- How to submit concerns about Bill C-27
- Road ahead – preparing for CPPA and AIDA

---

1 The Council of Canadian Innovators is the 21st century business council exclusively focused on helping high-growth Canadian technology firms scale-up globally. The Council's mandate is to optimize the growth of Canada's innovation-based sector by ensuring Canadian tech and public-policy leaders are working together to improve Canada's innovation outputs. To learn more about the CCI, click here.

Background to Bill C-27

- On June 16th, ISED Minister Champagne introduced Bill C-27, the *Digital Charter Implementation Act*, 2022.
- Bill C-27 will likely go to either the ETHI Committee or the INDU Committee in the Fall.
- If passed, Bill C-27 will:
    - replace and modernize the current federal private sector privacy law under PIPEDA with the *Consumer Privacy Protection Act* (**CPPA**);
    - create a new Personal Information and Data Protection Tribunal (**Tribunal**) with responsibility to impose administrative monetary penalties (**AMPs**) and fines; and
    - enact the *Artificial Intelligence and Data Act* (**AIDA**).
- On June 23rd, Philippe Dufresne was appointed Canada's new Privacy Commissioner effective June 27th.

Summary of Bill C-27

- Like PIPEDA, the CPPA:
    - provides principles-based rules that are technology-neutral, apply across sectors, and are grounded in a primacy-of-consent framework;
    - balances the interests of individuals and organizations;
    - does not expressly recognize privacy as a fundamental human right; and
    - does not expressly apply to federal political parties and politicians.
- See: New Privacy Bill: CPPA 2.0 - plus oversight of artificial intelligence,
    - *DYL Compliance Bulletin*, June 2022
- Unlike PIPEDA, the CPPA includes:
    - reinforced valid consent requirements with important new exceptions (that include an organization collecting and/or using an individual's personal information (**PI**), without their knowledge or consent, for certain "business activities" and "legitimate interests" of the organization or an organization disclosing PI to certain public institutions for defined "socially beneficial purposes";
    - increased flexibility and clarity for businesses (that include providing for codes of practice and certification programs, defining "de-identified" information and allowing for limited uses of it, and stipulating that the law does not apply to "anonymized" information);
    - clearer accountability requirements (for privacy management programs and service providers);
    - new individual rights (of data mobility, data disposal, and explanation of automated decision systems); and

- new enforcement powers and tools (including new order-making powers for the Privacy Commissioner, potentially onerous AMPs and fines, and a limited private right of action (**PRA**) for affected individuals).

Accountability

An organization:

- is accountable for PI under its control (s. 7(1));
    - PI is "under the control" of the organization that decides to collect it and that determines the purposes of its collection, use or disclosure (s. 7(2));
    - even if the organization transfers PI to a service provider, control remains with the organization; and
- must designate an individual to be responsible for its compliance under the CPPA (e.g., a privacy officer) (s. 8) and must provide that designated individual's business contact information to anyone who requests it.

Privacy management programs

- Organizations must implement and maintain a privacy management program (**PMP**) that includes the organization's policies, practices and procedures (**PPPs**) to fulfill its CPPA obligations respecting (s. 9(1)):
    - protecting PI;
    - receiving and dealing with requests for information and complaints;
    - providing training and information to staff; and
    - developing materials to explain its policies and procedures.
- Unlike PIPEDA, the CPPA requires organizations to
    - take into account the volume and sensitivity of the PI under its control when developing its PMP (s. 9(2)); and
    - on the Privacy Commissioner's request, give the Commissioner access to an organization's PPPs (s. 10(1)).
        - after reviewing the PPPs, the Commissioner may provide guidance on, or recommend corrective measures be taken in relation to, the organization's PMPs. But the Commissioner cannot use such accessed PPPs to initiate a complaint or carry out an audit unless the organization willfully disregards the Commissioner's recommendations (s. 111).

Reinforced conditions for valid consent

- The following elements must be provided in plain language at or before the time an individual's consent to collection, use or disclosure of their PI is sought (ss. 15(1), (2), (3) and (4)):
    - the purposes for which PI is collected, used or disclosed;
    - the manner in which PI is collected, used or disclosed;

- any reasonably foreseeable consequences of the collection, use or disclosure of the PI;
- the specific type of PI that is to be collected, used or disclosed; and
- the names of any third parties or types of third parties to which the PI may be disclosed.

- Consent must be expressly obtained unless it is appropriate to rely on implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the PI (s. 15(5)).

Exception to consent

- The CPPA is a primacy-of-consent privacy law, subject to many exceptions.
- Sections 18 – 51 stipulate the exceptions that are available:
  - Business Operations;
  - Public Interest;
  - Investigations;
  - Disclosures to Government Institutions;
  - Disclosures Required by Law; and
  - Publicly Available Information.

"Business activities" exception to consent

- An organization's collection or use of an individual's PI for certain "**business activities"*** does not require the individual's knowledge or consent provided that:
  - a reasonable person would have expected the collection or use; *and*
  - the information is not collected or used for purposes of influencing behaviour – in other words, not for tracking or automated processing for targeting purposes (s. 18(1)).

  ***Excepted business activities are those necessary (s. 18(2)):

  (a) to deliver a product/service requested by the individual,

  (b) for the organization's information, system or network security,

  (c) to ensure the safety of a product/service delivered by the organization, and

  (d) for any other activity prescribed by the CPPA regulations (**Regs**).

"Legitimate interest" exception to consent

- An organization may collect or use an individual's PI without their knowledge or consent if the collection or use is made for the purpose of an activity in which the organization has a "**legitimate interest**" that outweighs any potential adverse effect on the individual resulting from that collection or use provided that:

- a reasonable person would have expected the collection or use; *and*
- the information is not collected or used for purposes of influencing behaviour (s. 18(3)).

- Before collecting or using PI under this exception, the organization must conduct and record a "privacy/legitimate interest risk assessment" (**PIA** or **LIA**) – specifically, it must:
  - identify any potential adverse effect on the individual that is likely to result from the collection or use;
  - identify and take reasonable measures to reduce the likelihood that the effects will occur or to mitigate or eliminate them;
  - comply with any requirements prescribed under the Regs (s. 18(4)); and
  - record its assessment and, on request, provide a copy to the Privacy Commissioner (s. 18(5)).

Obligations of service providers

- A service provider is defined as an organization (including a parent/subsidiary/affiliate company) that provides services for another organization to assist in fulfilling its purposes.
- Service providers are generally not subject to Part 1 of the CPPA (the "obligations of organizations"), with some exceptions (s. 11(2)) namely:
  - security safeguards (s. 57); and
  - notification to customer in case of a breach of security safeguards (s. 61).
- However, the service provider is subject to all of the Part 1 obligations of organizations if it collects, uses or discloses that PI for any purpose other than the purpose for which the PI was transferred.
- An organization may transfer PI to a service provider without an individual's knowledge or consent (s. 19).
- An organization must ensure, by contract or otherwise, that its service provider provides a level of protection of the PI equivalent to that which the organization is required to provide under the CPPA (s. 11(1)).

Cross-border transfers of PI

- The CPPA applies in respect of PI that is collected, used or disclosed interprovincially or internationally (s. 6(2)).
- Transparency requirement - privacy policy must include details as to whether or not the organization carries out any international or interprovincial transfer or disclosure of PI but only if the transfer or disclosure may have "reasonably foreseeable privacy implications" (s. 62(2)(d)).
- Contrast Quebec's recently amended privacy law (Bill 64 aka Loi 25) where there is a requirement for a PIA with respect to the protection of PI in the foreign jurisdiction.

Codes of practice and certification programs

- Are statutorily recognized under the CPPA and allow for voluntary accountability frameworks.
- Any organization may seek the Privacy Commissioner's approval of codes of practice and certification programs (ss. 76 and 77).
- A code of practice must provide for substantially the same or greater protection of PI as under the CPPA.
- Process and criteria for Privacy Commissioner's approval of codes of practice and certification programs will be set out in the Regs.
- To be approved, an entity's certification program must include a code of practice, guidelines for interpreting and implementing the code, a mechanism for certifying compliance with the code, disciplinary measures for non-compliance, and anything else set out in the Regs.
- An organization can decide to voluntarily comply with the code and maintain its certification under the program.
- While certification does not necessarily ensure CPPA compliance, the Privacy Commissioner has discretion to not investigate a certified organization (s. 83(1)(d)) and may not recommend that an AMP be imposed on an organization (s. 94(3)), if the Privacy Commissioner is of the opinion that, at the time of the CPPA contravention, the organization was certified under the program and was in compliance with the requirements of that program.
- A potential significant role for codes of practice may be in articulating detailed standards for protecting de-identified information and defining more explicitly anonymized information.
    - For example, see ongoing work of CIO Strategy Council such as draft CAN/CIOSC 100-3: Data Governance – Part 3 Privacy enhancing de-identification framework.

De-identification and Anonymization

- The CPPA sets forth a regime addressing the use and disclosure of non-identifiable information that aligns with the GDPR and Quebec's Bill 64/Loi 25.
- It clarifies that de-identified information is considered PI subject to the CPPA (with the exceptions described below) and anonymized information is largely outside the CPPA.
    - *De-identified information* is defined as PI that has been modified so that an individual cannot be directly identified from it, recognizing that a risk of re-identification remains.
    - *Anonymized information* is defined as PI that has been irreversibly and permanently modified, in accordance with generally accepted best practices, to ensure that no individual can be identified from the anonymized information, whether directly or indirectly, by any means.
- De-identified information is PI subject to all the CPPA's provisions except that an organization may:

- use an individual's PI without their knowledge or consent (a) to de-identify it (s. 20), (b) for the organizations' internal research, analysis and development purposes (s. 21), and (c) for due diligence in prospective business transactions (s. 22(1); and
- disclose (to a government, health care, or post-secondary educational institution, public library or other public institution mandated/prescribed by the Regs) an individual's PI without their knowledge or consent for "socially beneficial purposes" (defined as purposes related to health, the provision/improvement of public amenities/infrastructure, environmental protection, or any other purpose prescribed by the Regs) (s. 39(1)).

- De-identified information is also excepted from the following CPPA provisions:
  - where an organization has received a request from an individual to dispose of their PI (s. 55);
  - where an organization must take reasonable steps to ensure PI under its control is correct/up-to-date/complete (s. 56);
  - where an organization has received a request from an individual for access to their PI (s. 63(1));
  - where an organization has received a request from an individual to amend their PI (s. 71(1));
  - where an organization has received a request from an individual to disclose the PI that organization has collected from the individual to another organization under a "data mobility framework" (s. 72);
  - where an organization de-identifies PI, it must ensure that the technical and administrative measures applied to the information are proportionate to the purpose for de-identifying the PI and the sensitivity of the PI (s. 74); and
  - where an organization is prohibited from using de-identified information (alone or in combination with other information) to identify an individual except (ss.75 and 116):
    - to conduct testing of the effectiveness of the organization's security safeguards;
    - to comply with requirements under the CPPA or under federal/provincial law;
    - to conduct testing of the fairness and accuracy of models, processes and systems that were developed using the de-identified information;
    - on request by an organization, for a purpose or situation authorized by the Privacy Commissioner where, in the Commissioner's opinion, the identification is clearly in the interests of the individual; and
    - in any other circumstances prescribed by the Regs.

Individual right to data mobility

- The right to data mobility provides individuals with the right of control over their data (opportunity for choice) but also to enhance competition amongst organizations.

- The mobility right will be enabled through the Regs providing for "data mobility frameworks", governing both sending and receiving organizations, and articulated by industry-specific standards and codes of practice (ss. 72 and 123).
- Such frameworks will provide for:
    - security safeguards for data when disclosed, received and in transit;
    - interoperability requirements;
    - verification of consent;
    - exceptions for confidentiality of technology; and
    - protection of IP rights.
- Data mobility will not apply to "derived data", only to the raw data collected from the individual – such derived data is considered organization-specific IP and confidential information.

Individual right to disposal

- The CPPA establishes a right of disposal – an obligation on an organization to dispose of an individual's PI that is under the organization's control, on that individual's request, subject to the following exceptions (s.55):
    - the information contains another individual's PI that is not severable;
    - the information is required by law or reasonable contract terms to be retained;
    - the information is required for legal defense/remedies purposes by the organization;
    - the information is not in relation to a minor and is required for the provision of a product or service to the individual requester;
    - the request is vexatious or made in bad faith; or
    - the information is not in relation to a minor and is scheduled to be disposed of per the organization's information retention policy and the organization tells the individual how much longer the information will be retained.
- The right does not expressly extend to the de-indexing of information such as on search engines.
- Contrast – Quebec's Bill 64/Loi 25 (which provides a right to de-indexation where the PI has been used contrary to law - e.g., for cyberbullying - or where the PI's public availability causes serious injury to an individual's privacy or reputation that is not outweighed by public interest - e.g., freedom of expression) and the GDPR (which provides for a global right to be forgotten limited only by freedom of expression and other public interest rules).

Individual right to explanation in automated decision systems

- The CPPA gives individuals the right to an explanation (also known as "**algorithmic transparency**"), regarding automated decision systems (**ADS**) – specifically:

- the right, on request by an individual, to get an explanation from the organization in plain language (ss. 63(3), 66(1)):
    - of any prediction, recommendation or decision based on ADS that could have a significant impact on the individual; and
    - how the PI used to make that prediction, recommendation or decision was obtained, the source of the information and the reasons or principal factors that led to that prediction, recommendation or decision.
- The CPPA defines ADS as technology that assists or replaces the judgement of humans using techniques like rules-based systems, regression analysis, predictive analytics, machine learning, deep learning, and neural nets.
- An organization using an ADS must make readily available, in plain language, a general account of its use of the ADS to make predictions, recommendations or decisions about individuals that could have a significant impact on them (s. 62(2)(c)).
- The CPPA does not expressly give individuals a right to contest ADS-based predictions, recommendations or decisions or to object to having their PI used (as recommended by the Privacy Commissioner in *A Regulatory Framework for AI: Recommendations for PIPEDA Reform* dated November 12, 2020).
- Under the GDPR (Art. 22), an individual has the right not to be subject to automated decision-making (if the decision produces legal effects or affects the individual and is solely based on automated processing, including profiling).

Increased risks for non-compliance – *New model, powers and tools*

- The CPPA
    - replaces PIPEDA's "ombudsperson" model with an "enforcement" model (akin to that under the federal *Competition Act*); and
    - gives the Privacy Commissioner new and stronger enforcement powers and tools.
- The CPPA does not give the Privacy Commissioner power to directly impose AMPs (unlike the power of European data protection authorities under the GDPR).
    - But the Privacy Commissioner may be able to include a financial payment by an organization under investigation/inquiry as part of a negotiated compliance agreement (s. 87).
- Under the CPPA, the Privacy Commissioner retains powers to:
    - investigate an organization's compliance (either on its own or in response to an individual's complaint) (ss. 82 and 83);
    - enter into compliance agreements with organizations that have, are about to, or are likely to contravene the CPPA (s. 87);
    - make rules respecting the conduct of an inquiry (s. 92); and
    - conduct audits (s. 97).
- Also under the CPPA, the Privacy Commissioner gets new powers to:

- discontinue an investigation or resolve a complaint through mediation (ss. 85 and 86);
- issue compliance orders (e.g., requiring organizations to take measures to comply with the CPPA or a compliance agreement or to make public measures to correct its privacy policies, practices or procedures (s. 93(2)), appealable to the Tribunal (s. 101); and
- make any interim order the Commissioner considers appropriate during an investigation, inquiry or audit (s. 99(1)(d)), appealable with leave to the Tribunal (s. 102(1)).

Increased risks for non-compliance – *Commissioner may recommend AMPs*

- If, on completing an inquiry, the Privacy Commissioner finds that an organization has contravened certain provisions of the CPPA, the Commissioner may recommend that the Tribunal impose an administrative monetary penalty (**AMP**) on the organization (s. 94(1)).
- In making the decision, the Privacy Commissioner must take into account (s.94(2)):
  - the nature and scope of the contravention;
  - any evidence that the organization exercised due diligence to avoid the contravention;
  - whether the organization made reasonable efforts to mitigate or reverse the contravention's effects;
  - the organization's history of compliance with the CPPA;
  - any prescribed factor; and
  - any other relevant factor.
- The Privacy Commissioner's decision not to recommend that a penalty be imposed on the organization may be appealed by the complainant to the Tribunal (s. 101).

Increased risks for non-compliance – *Tribunal may impose AMPs*

- The CPPA gives the Tribunal power to impose, on recommendation of the Privacy Commissioner, potentially onerous AMPs (s. 95(4)):
  - Max: the higher of $10 million and 3% of organization's gross global revenue in last financial year, for the following contraventions:
    - collecting PI in a manner and for purposes beyond those necessary and identified and recorded by the organization (ss. 12(1) and 13);
    - using or disclosing PI for a secondary purpose without consent (s. 14(1));
    - contravening the "refusal to deal" provisions (s. 15(7));
    - obtaining consent through deception (s. 16);
    - contravening the "legitimate interest" provisions (ss.18(3), 18(4) and 18(5));

- contravening the retention (s. 53) and disposal (ss. 55(1), 55(3) and 55(4)) requirements or the safeguarding requirements (s. 57(1)); and
- failing to report a breach of security safeguards (s. 58(1)) or to notify affected individuals of breach of security safeguards (s. 58(3)).

- But the Tribunal must not impose an AMP if the organization establishes it exercised due diligence to prevent contravention (s. 95(3)).
- The Tribunal must consider several factors when imposing an AMP including (s. 95(5)):
  - the organization's ability to pay the AMP;
  - the AMP's likely effect on the organization's ability to carry on its business; and
  - any financial benefit the organization obtained from the contravention.

Increased risks for non-compliance – *Court may impose fines*

- The CPPA permits potentially onerous fines on conviction in court of an offence (s. 128).
  - Max: for indictable offences, the higher of $25 million and 5% of organization's gross global revenue in its last financial year.
  - Max: for summary conviction offences, the higher of $20 million and 4% of the organization's gross global revenue in its last financial year.
- These offences include:
  - failing to report a privacy breach that it is reasonable to believe creates a real risk of significant harm to an individual (s.58);
  - failing to keep and maintain a record of every breach of security safeguards involving PI under its control (s.60(1));
  - obstructing an investigation, inquiry or audit (s.128);
  - failing to retain PI that is subject to an access request (s.69);
  - using information that has been de-identified to identify an individual (s.75);
  - contravening a compliance order (s.93(2)); and
  - retaliating against a whistleblower (s.127(1)).

Increased risks for non-compliance – *Private right of action (PRA)*

- The CPPA gives affected individuals a limited PRA for damages for loss or injury as a result of a CPPA contravention in only two circumstances (s. 107):
  - where either the Privacy Commissioner or the Tribunal finds that the organization has contravened the CPPA (and the finding may no longer be appealed); and
  - where the organization has been convicted of an offence under the CPPA.
- Actions may be brought in Federal Court or any provincial superior court (s.107(4)).

- But they must be started within two years after the date of the Privacy Commissioner's finding, the Tribunal's decision (if there is an appeal) or the organization's conviction of a CPPA offence (s.107(3)).
- **Note:** The PRA is limited in that it requires a prior final finding by the Privacy Commissioner or Tribunal of contravention or conviction.

Oversight of high-impact AI systems – *Artificial Intelligence and Data Act* (AIDA)

- A significant provision of Bill C-27 is the proposed enactment of AIDA, intended to establish an oversight regime for "high impact" AI systems with a view to preventing harmful effects such as bias, physical and psychological health consequences, and economic loss resulting from their use.
- AIDA is intended to apply to *AI systems* "related to human activities" that qualify as "high impact" – which will be defined by regulations.
- Organizations operating such systems will be required to conduct risk assessments and undertake measures to mitigate risks identified by such assessments.
- The objectives of AIDA are in line with similar initiatives internationally, most prominently in the EU, which is proposing the *Artificial Intelligence Act* (**AI Act**) that would regulate "high risk systems" and prohibit stipulated AI systems having unacceptable consequences.

AIDA – Scope of Application

- Scope of application is intended to be narrower than the CPPA's application to ADS, focussing on autonomous or semi-autonomous systems that qualify as high impact.
- Under AIDA, an *AI system* is defined as:
  - a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.
- By contrast, the CPPA's rules apply to transparency for all *ADS systems*, which are defined as:
  - technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique.

Enforcement under AIDA

- An Artificial Intelligence and Data Commissioner is to be appointed to support the Minister in fulfilling responsibilities under AIDA, including by monitoring compliance, ordering third-party audits, and sharing information with other regulators as appropriate.
- Potential sanctions:
  - order-making powers enforceable as orders of the Federal Court (ss. 13-18, 20);
  - administrative monetary penalties – to be provided for in regulations (s. 29(1)); and

- fines for organizations depending on the offence up to a maximum of the greater of
    - $10 million or 3 per cent of global gross revenues for non-compliance with AIDA (ss. 6-12 and 30) or
    - $25 million or 5 per cent of global gross revenues for possession or use of illegally obtained personal information or for illegally making an AI system available for use (ss. 38, 39 and 40).

Comparisons to privacy laws in Europe

- The GDPR is a rights-based privacy law, which broadly contrasts with the principles-based approach of the CPPA (and PIPEDA).
- Significantly, it acknowledges the right to privacy as a "fundamental right" of individuals as laid down by the EU's *Charter of Fundamental Rights*, but also recognizes that this right must be balanced, in accordance with the principle of proportionality, with other rights including the right to freedom of expression and the right to conduct a business.
- Some view the more principles-based approach of PIPEDA and the CPPA as providing more flexibility than the more prescriptive and directive approach of the GDPR. But others see this as a false dichotomy.
- Moreover, the GDPR's *lawful-basis-for-processing* approach may provide a more flexible approach to evolving digital markets and innovation generally than PIPEDA's and the CPPA's *primacy-of-consent-with-exceptions* approach.
- Still, in many respects, the CPPA moves Canada's privacy law closer to the GDPR, including:
    - greater enforcement powers (order-making and financial penalties);
    - a reinforced and more rigorous consent rule;
    - new individual rights to data mobility, disposal, and explanation of ADS; and
    - a rule of proportionality balancing loss of privacy against the benefits of collecting or using PI including the "legitimate interest" of an organization.

Key differences from old Bill C-11

- From an organization's standpoint, Bill C-27 (2022) differs from Bill C-11 (2020) in several important respects, including:

    Accountability

    - the Privacy Commissioner has a new power to recommend corrective measures for an organization's privacy management program (s. 10(2));
    - the sensitivity of PI is a new factor for determining the length of an organization's data retention period (s. 52(2));

    Consent and Exceptions

    - organizations must rely on express consent (i.e., they may not rely on implied consent) to collect or use PI in the context of "business activities"

or they must satisfy the requirements of the "business activities" exception (s. 15(6));

- organizations may rely on the new "legitimate interest" consent exception provided they satisfy all of the associated conditions including carrying out and recording an LIA (ss. 18(3), (4) and (5));

Individual Rights

- individual rights may not apply to de-identified information (s. 2(3))*****;

  *******This point will likely be discussed at the parliamentary committee considering Bill C-27*

- for the right to disposal, there are new conditions (s. 55(1)) and exceptions (s. 55(2)); the requirement to provide an individual with an explanation of an ADS applies only to a prediction, recommendation or decision that could have a significant impact on the individual (s. 63(3));

De-identification and Anonymization

- a revised definition of "de-identify" and a new definition of "anonymize" (s. 2);
- explicit recognition that the CPPA does not apply to PI that has been anonymized (s. 6(5)) and more exceptions to the prohibition on re-identifying de-identified PI (s. 75);
- an organization may request the Privacy Commissioner's authorization to re-identify an individual from de-identified information if the Commissioner believes it is clearly in the individual's interest (s. 116);
- the consent exception for an organization's internal use of de-identified PI for "research" and "development" has been extended to "analysis" (s. 21);

Enforcement

- contraventions of the following CPPA provisions are now subject to penalties (s. 94(1)):
  - privacy management program (s. 9);
  - transfers to service providers (s. 11);
  - purpose limitation (ss. 12(3) and (4));
  - obtaining consent (s. 15(1));
  - forcing consent when not a condition of service (s. 15(7));
  - consent by deception (s. 16);
  - withdrawal of consent (s. 17(2));
  - retention (s. 53);
  - service provider breach notification (s. 61); and

        - making available information about privacy policies and practices (s. 62(1)).
    - the Privacy Commissioner must take into account new factors when deciding whether to recommend a penalty be imposed by the Tribunal (s.94(2)):
        - evidence that the organization exercised due diligence to avoid the contravention;
        - whether the organization made reasonable efforts to mitigate/reverse the contravention's effects; and
        - any other factor prescribed by the Regs.

Key takeaways for Canadian businesses

- New risks:
    - greater legal and financial risks for non-compliance;
    - potentially high and onerous AMPs and fines; and
    - using AI technologies will require complying with a new obligation to explain specific predictions, recommendations and decisions in plain language.
- New opportunities:
    - broader consent exceptions for certain business activities and socially beneficial purposes;
    - prospects for co-regulatory industry codes of practice and certification programs; and
    - greater flexibility to use de-identified and anonymized information.
- Implement and maintain a robust privacy management program.
- Document CPPA compliance by conducting data mappings and privacy impact assessments and documenting compliance checks on service providers (helps establish "due diligence" defense).
- Update privacy policies and consents keeping in mind the new requirements for providing certain information in "plain language" (which includes mentioning the reasonably foreseeable consequences of the PI's collection, use and disclosure).
- Review/enhance internal procedures and data mapping in order to be able to respond to individual's requests to include protecting an individual's right to be informed of AI, right to require an organization to dispose of their PI, and the right to data mobility.

How to submit concerns about Bill C-27

- The Federal Government has not given any timetable for the parliamentary committee hearings or whether Bill C-27 would be reviewed by the ETHI Committee or the INDU Committee; however parliamentary committee review is expected to commence in the Fall.
- If stakeholders have questions/concerns, they should contact ISED:

    - Jill Paterson, Acting Director, Privacy and Data Protection Policy, Marketplace Framework Policy Branch (Jill.Paterson@ised-isde.gc.ca).
- Or seek an invitation to appear before the parliamentary committee once hearings begin.

Road ahead for transition to CPPA and AIDA

- There will be a transitional period for businesses to comply after the CPPA comes into force.
- It is reasonable to expect that this transition period will be at least 15-18 months.
- Many provisions will require regulations before becoming operative; process likely will involve consultation and publication of draft regulations before becoming final, which may extend the coming-into-force status of certain provisions of the CPPA and AIDA.

Disclaimer and Questions

This briefing provides only general information about Bill C-27. It is not legal advice. If you have any questions, please contact Bill Hearn at bhearn@foglers.com or David Young at david@davidyounglaw.ca. Thank you.