Understanding Key Features proposed in the Consumer Privacy Protection Act (CPPA)

The information contained in this document has been compiled from ongoing discussions with IAB Canada legal counsel, government representatives and business privacy professionals. Its purpose is to act as an initial resource while we continue to assess the Act and gain clarity on the details of the regulations.

Key Feature of CPPA	Overview	Details
Enforcement & Order Making Powers	The CPPA introduces an **enforcement regime** with potentially severe **financial penalties**, a **private right of action** and **order making power** for the Privacy Commissioner of Canada.	**Enforcement Regime** Introduction of an enforcement regime with highest fines in the G7. Under the draft CPPA, the Privacy Commissioner may recommend to the Tribunal that a penalty for contravention of the various obligations in the CPPA be imposed on the organization. The maximum penalty is the higher of $10 million or 3% of gross global revenue. Penalties may only be imposed by Tribunal for certain contraventions including: • collecting personal information beyond that which is necessary for purposes identified and recorded by an organization • using or disclosing personal information for a secondary purpose without consent • contravening the "refusal to deal" provision • obtaining consent through false or misleading information, or using deceptive practices • contravening the retention and disposal requirements • contravening the safeguarding requirements • failing to report breach of security safeguards • failing to notify affected individuals of breach of security safeguards Certain ***knowing*** contraventions may be prosecuted as offences in court including: • failing to report breach of security safeguards or notify affected individuals • failing to provide Commissioner with access to breach records • failing to retain personal information that is subject of personal information request • using de-identified information to identify an individual • retaliating against a whistleblower • obstructing an investigation, inquiry or audit

		Private Right of Action • An expansion on the private right of action under PIPEDA, the CPPA also establishes a cause of action for loss or injury arising from an organization's contravention of its obligations under the legislation. The CPPA extends the limitation period to two years after the day on which the individual (who is affected by an act or omission by an organization that constitutes a contravention of the CPPA) becomes aware of: ◦ the relevant decision of the Privacy Commissioner (or in the event of an appeal, of the Tribunal's decision), with respect to such act or omission; or ◦ a conviction under the indictable offence section. The private right of action may extend to service providers to the extent there is a finding that they failed to comply with their obligations under the CPPA. **Order Making Powers for Commissioner** • During an investigation, inquiry or audit, the Privacy Commissioner may, make any interim order that the Commissioner considers appropriate. Following an inquiry, Commissioner may **order an organization to comply and to publicize corrective measures.** • After investigating a complaint (either initiated by a complainant or the Privacy Commissioner), the Privacy Commissioner may conduct an inquiry and render a decision and order the organization to take specific steps, cease taking any particular action (such as collecting information) and recommend that the Tribunal impose a penalty in respect of certain contraventions (as detailed below). • Compliance orders may be appealed to the Tribunal, but the Tribunal will only replace its finding of fact for that of the Privacy Commissioner based on a palpable and overriding error standard. In effect, this standard means that the Tribunal will defer to findings of fact by the Privacy Commissioner.
Transparency	Organizations are required to make information that explains its policies and practices readily available in "plain language."	There are several new content requirements within the CPPA that supplement PIPEDA's existing transparency requirements. Organizations are now required to provide: • A general account of any automated decision systems that could have a significant impact on individuals. • How they apply consent exceptions to its practices. • Whether or not they transfer or disclose information internationally or interprovincially in a way that may have reasonably foreseeable privacy implications. • How individuals may make a request for the disposal (permanent and irreversible deletion) of their information.

Reasonable and Appropriate Provisions for Collection, Use and Disclosure	The CPPA restates the "reasonable and appropriate" provision whereby an organization may only "collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances"	Mandatory factors to consider in determining whether purposes are appropriate include: • the **sensitivity** of the personal information. • whether the purposes represent **legitimate business needs** • the **effectiveness** of the collection use or disclosure in meeting the organization's legitimate business needs. • whether there are **less intrusive means** of achieving those purposes at a **comparable cost** and with **comparable benefits**; and • whether the individual's **loss of privacy** is **proportionate to the benefits** in light of any measures, technical or otherwise, implemented by the organization to mitigate **the impacts of the loss of privacy** on the individual.

Purpose Identification & Data Minimization	CCPA states that organizations must **identify** and **record** the purposes associated with personal information that they collect, used or disclose **at or before the time of collection**, or before using or disclosing for a new purpose going beyond PIPEDA which requires that organization document only the purposes of collection.	• Organizations may only collect the personal information **that is necessary** for the determined and recorded purposes.
		  ○ The concept of "necessary" has been interpreted as akin to "required", and a higher standard than PIPEDA's "mere reasonableness"
		  ○ Operationalizing this principle within complex data ecosystems, AI contexts, etc. may prove very challenging
		• If an organization contravenes the limitation of collection requirements penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues.

Consent	The CPPA reinforces consent (especially express consent) as the primary authority for organizations to **process** personal information, and more **prescriptive** consent **requirements**.	• The CPPA provides that express consent is the default form of consent and that an **implied form of consent** may only be relied upon if the **organization establishes that it is appropriate to rely on an individual's implied consent**, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed. **Valid Consent** The CPPA states that an organization must obtain an individual's **valid consent** for the collection, use or disclosure of the individual's personal information unless otherwise provided by the law.

		The CPPA provides prescriptive information requirements for a valid consent which are:
		
		• The information must be **provided** in **plain language** at or before the time the individual seeks the consent.
		• The information must include the following content
		  ○ (a) the **purposes for the collection, use or disclosure** of the personal information determined by the organization and recorded under the Act's "appropriate purposes" provisions
		  ○ (b) **the way in which the personal information is to be collected, used or disclosed**.
		  ○ any **reasonably foreseeable consequences** of the collection use or disclosure of the personal information.
		  ○ the **specific type of personal information** that is to be collected, used or disclosed; and
		  ○ the **names of any third parties or types of third parties** to which the organization may disclose the personal information.
		
		Withdrawal of Consent
		
		• Upon receiving notice of withdrawal of consent from the individual, an organization must **inform the individual of the consequences of the withdrawal** of their consent, and **"as soon as feasible after that" cease the collection, use or disclosure** the applicable personal information.
		
		If an organization contravenes the consent requirements penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues.
		
		Exceptions for consent
		Organizations may collect and/or use personal information without consent in the course of standard business operations such as:
		
		• to **transfer personal information to their third -party service providers**.
		• to process of **de-identifying personal information**.
		• to collect and use (**but not disclose**) of personal information for a broad range of standard "business activities" including an activity:
		  ◦ **necessary to provide or deliver a product or service** that the **individual has requested** from the organization
		  ◦ carried out in the **exercise of due diligence to prevent or reduce the organization's commercial risk**.
		  ◦ **necessary for the organization's information, system or network security**.
		  ◦ necessary for the **safety of a product or service** that the organization provides or delivers.

		◦ in the course of which **obtaining the individual's consent would be impracticable** because the organization **does not have a direct relationship** with the individual. **<u>provided that</u>** in the course of any activity: • the collection or use is something a **reasonable person would expect**; and • the collection or use **is not used to influence the individual's behaviour or decisions**. Organizations may also collect and/or use personal information without consent for the broad concept of "internal research and development purposes", but only if the i**nformation is "de-identified" prior to the use** for such purpose. Many wholly R&D activities that legitimately require the processing of personal information (including standard customer research, AI and other complex analytics) will fall outside the scope of this exception to consent authority. **Use and Disclosure or Research Purposes:** The CPPA maintains an exception to consent for disclosure of personal information for "statistical purposes or scholarly study or research purposes**,** provided that: • those purposes cannot be achieved without disclosing the information. • it is impracticable to obtain consent; and the organization informs the commissioner before the disclosure.
Accountability	The CCPA states that organizations are **"accountable"** for personal information under its control. It also sets out provisions that clarify the concept of an **"accountable organization"** and several provisions relating **to "demonstrable" accountability.**	Personal information is under the control of an organization that **decides to collect it and that determines the purposes** for its collection, use or disclosure, regardless of whether the information is collected, used or disclosed by the organization itself" or by a service provider CPPA requires organizations to implement a **privacy management program**, which must: • include **policies, practices and procedures** that are put in place to fulfil the organization's obligations under the Act and • **take into account the volume and sensitivity** of personal information under the organization's control. **Upon request of the Commissioner (no reasonable grounds necessary), organizations are required to provide the Commissioner with access to their policies, practices and procedures that are included in its privacy management program.** CPPA will require an organization to identify and record each of the purposes for which it collects, uses, or discloses any personal information, and that it do so at or before the time of collection. In this respect, the CPPA appears to go beyond PIPEDA, which requires that organizations document only the purposes.

Accountability Frameworks – Codes and Practice Certifications	The CPPA **provides statutory recognition** of codes of practice and related certification programs.	This allows for the establishment of voluntary accountability frameworks that may be very helpful for personal information processing in complex data ecosystems, sectoral information sharing arrangements, AI and other complex analytics and business models. The act states that: • Codes of practice need to provide for "substantially the same or greater protection of personal information as some or all of the protection provided" under the Act. • Criteria for codes and certification programs to be set out in regulations. • Organizations would apply to the Commissioner for approval of a code or program, and Commissioner has to make public his/her decision. • Compliance with a code does not relieve an organization of its obligations under the Act. • Certification programs run by entities will include independent verification mechanisms and disciplinary measures for non-compliance with the code. **The Commissioner's powers include:** • Cooperating with an entity that operates a program for the exercise of the Commissioner's powers and duties. • Revoking an approval. • Discretionary power to decline to investigate a complaint when it "raises an issue in respect of which a certification program that was approved by the Commissioner… applies and the organization is certified under that program." • **Commissioner <u>cannot</u> recommend a penalty if an organization is in compliance with an approved code or certification program BUT the private right of action would still be available.**
Right of Disposal	The CPPA creates a **new statutory right** for individuals to have their personal information **disposed** by the organization in control **upon request.**	This statute contains the following key requirements and features: • the disposal must result in the "permanent and irreversible deletion of personal information". • Based on existing wording, the right of disposal is not restricted to just personal information "online". • The disposal must take place "as soon as feasible" after the request. • The organization who receives the request must inform any service provider as soon as feasible and obtain a confirmation of the individual's request from the service provider. ◦ Grounds for refusing such disposal will be limited to situations where it would result in disposing of information about another individual or where

		federal, provincial or contractual requirements would prevent the organization from doing so. • Where an organization refuses an individual's request, an organization must inform the individual in writing and set out the reasons and any recourse the individual may have to challenge compliance. **If an organization contravenes the retention and disposal requirements penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues.**
Data Mobility Rights	The CPPA introduces a concept of **data mobility rights** which creates a limited right to data portability, which will **allow** individuals to **request** from an organization in control that their personal information be **disclosed** to **another organization**	Key requirements for data mobility rights include: • The data mobility disclosure must take place "as soon as feasible" • Both organizations must be subject to a "data mobility framework" provided under the regulations of the Act Key details about the nature, scope and requirements of data mobility rights will be set out in regulations that may include: • data mobility frameworks that provide ◦ safeguards to enable the secure disclosure and subsequent collection of the personal information and ◦ parameters for the technical means for ensuring interoperability in respect of the disclosure and collection of that information. • requirements that specify organizations that are subject to the data mobility framework and • requirements that provide for exceptions to the data mobility disclosure requirement, including exceptions related to the protection of proprietary or confidential commercial information.
Provisions for Automated Decision-Making Systems	CPPA defines an "automated decision system," as: "any technology that assists or replaces the judgement of human decision-makers using techniques such as **rules-based systems**, **regression analysis**, **predictive analytics**, **machine learning**, **deep learning** and **neural nets**."	The CCPA outlines new requirements for these systems which include: • Openness: Organizations must make available a **general account of the organization's use of any automated decision system** to make predictions, recommendations or decisions about individuals **that could have significant impacts** on them. • Access: Organizations have an explicit obligation to, **upon request**, **provide individuals with an explanation of any prediction, recommendation or decision made by an automated decision system**, and of **how the personal information that was used** to make the prediction, recommendation or decision was obtained. This information must be provided in **plain language**.

De-Identified Data	CPPA includes several technical provisions involving the process of de-identification of personal information, and the use and disclosure of de-identified data.	In CPPA, "de-identify" is defined in the statute as a "means to modify personal information — or create information from personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual." There is clarity required as to whether sufficiently "de-identified" data is still "personal information" for the purposes of the CPPA. The bill contemplates rules protecting "personal information", but in certain circumstances, the statute regulates the use or disclosure of "de-identified" data (i.e., not PI). **This is an area of concern and being taken up with the regulators to gain clarity.** **Requirements for De-Identification Process:** • In the course of the de-identification process, organizations are obligated to ensure that any **technical and administrative measures** applied to the information are **proportionate to the purpose** for which the information is de-identified **and the sensitivity** of the personal information. **Authorized Uses of De-identified Data:** The concept of "de-identifying" data is incorporated as a condition in circumstances for an organization to use or disclose personal information without consent. (see section on exceptions for consent) **Authority to De-Identify:** • The CPPA helpful clarifies that organizations are legally authorized under the statute to de-identify data without obtaining the consent of the individual to whom the personal information relates. **Prohibitions on Re-identification:** • Under CPPA it is prohibited to use de-identified information - alone or in combination with other information - to identify an individual, except in order to conduct testing of the effectiveness of security safeguards that the organization has put in place to protect the information. ***Knowingly* using de-identified information in contravention may be prosecuted as an offence in court and the organization could be liable for a fine of up to the higher of $25 million or 5% of gross global revenues.**
Breach Notification Requirements	Similar to within PIPEDA, the CPPA clarifies that **service providers** are required to notify the **organization that controls the personal information** of a breach of security safeguards.	• If an organization contravenes the breach notification requirements or the safeguarding requirements within the CPPA, penalties may be imposed by the Tribunal and the organization could be liable for a fine of up to the higher of $10 million or 3% of gross global revenues. • If an organization **knowingly** contravenes these requirements, the contravention may be prosecuted as an offence in court and the organization could be liable for a fine of up to the higher of $25 million or 5% of gross global revenues.