Feedback: 2026 Review of the Privacy Act - Policy approaches[1]

Theme 1: Enabling integrated services

1. Do you agree with the approach overall?

Somewhat disagree

BCCLA supports making services easier to access, but the *Privacy Act* should not become an enabling statute for whole-of-government data integration. Any service integration must be subordinate to privacy, dignity, autonomy, equality, democratic participation, and freedom from state surveillance. In particular, it is important to recall that the right to informational privacy protected by section 8 of the *Charter* hinges on an individual's autonomy over information about themselves: "to determine for themselves when, how, and to what extent information about them is communicated to others" (R v Tessling, 2004 SCC 67 at para 23).

The proposals regarding Theme 1 appear to put administrative efficiency first, convenience second, and rights-protective limits last. E.g., the integrated services model is presented as universal, with no requirement that an individual consent to participating in it, nor any opportunity for the individual to remove themselves from the regime.

Any integrated-service model should: require clear legal authority for disclosure; meet standards for necessity, proportionality, effectiveness, and least-intrusive means; require written data-sharing agreements that are published to the public; be thoroughly examined through regularly-updated privacy impact, human-rights, and equality assessments; maintain clear audit trails of information disclosure; have strict deletion rules; provide meaningful notice of information

[1] Government of Canada: 2026 Review of the Privacy Act: Policy Approaches, available online: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/privacy-act-modernization-policy-approaches/2026-review-privacy-act-policy-approaches.html

British Columbia Civil Liberties Association
306 – 268 Keefer Street
Vancouver. BC, Canada V6A1X5
Tel 604.687.2919
Fax 604.687.3045
Toll-free 1.855.556.3566
info@bccla.org
www.bccla.org

disclosures; and be opt-in so that individuals can exercise their autonomy over information about themselves.

Secondary use of collected data for policing, immigration enforcement, national security, intelligence, benefit-fraud analytics, or other punitive purposes should be prohibited unless specifically authorized by clear and specific legislation and subject to independent meaningful review. For a review to be meaningful in this context, it must be timely and have enforceable outcomes to protect the privacy of the person impacted.

Modernization must close interjurisdictional gaps. Where information moves between federal, provincial, territorial, municipal, Indigenous, educational, policing, health, transportation, or social-service bodies, privacy protections should follow the information end-to-end, rather than changing depending on which institution happens to hold it at a particular moment.

2. Do you agree that government institutions should be allowed to securely share and reuse personal data across programs and levels of government without asking for consent, where doing so serves a public interest or benefits individuals (for example, to improve service delivery or program operations) and is subject to strong privacy safeguards? (See proposal 1)

Disagree

This proposal aims to eliminate the "siloed model" of separate data collection and retention by different public bodies on the grounds that it creates inefficiencies. This may be true, but decentralized silos of information are also protective: the more centralized are government holdings of personal information, the greater the consequences of a breach will be. Mere efficiency or the reduction of overhead is insufficiently pressing and substantial an objective to justify infringement of *Charter*-protected informational privacy rights, as disclosure of personal information between public bodies without consent would do, nor does it justify increasing the risk to individuals by putting all their informational eggs in one government basket.

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

The power dynamics that exist between the state and those subject to its jurisdiction and reliant upon it for basic services often prevent or impair an individual's ability to meaningfully consent. In a free and democratic society, this unhappy dynamic is a reason to further empower the individual, not a licence to disregard consent and autonomy altogether.

Broad administrative discretion to reuse personal data without the consent of those the data concerns is fundamentally incompatible with the autonomy required for informational privacy. The proposed requirements for disclosure – "public interest" and "benefits individuals" – are inappropriately broad, open-ended, and subjective in their ordinary senses. If they are used, they must be defined narrowly, with statutory criteria that must be met, including a requirement for evidence that the sharing is necessary for the public body's program, proportionate, effective, and the least intrusive option.

Non-consensual disclosure between public bodies should further require a written agreement identifying the legal authority, purpose, data elements, recipients, onward-sharing limits, retention, security, audit logs, breach obligations, complaint routes, and consequences for non-compliance. Such written agreements must be available to the public.

Any high-risk disclosure, such as that of sensitive information, should require that privacy impact, human rights, and equality assessments are conducted and reviewed by the Privacy Commissioner, and that these assessments and a report by the Commissioner are made public in advance of implementation.

The *Charter* and the principle of rule-of-law require, at minimum, that any law that proposes to enable law enforcement, border security, or intelligence agencies access to personal information without a person's consent or judicial authorization must be subject to rigorous public scrutiny and open debate through the ordinary Parliamentary process, not through Cabinet choices made behind closed doors pursuant to a regulation making power. The *Act* should prohibit punitive or enforcement-related secondary use altogether, rather than exempting these purposes from the requirements that apply to interbody disclosure for other purposes.

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

For interjurisdictional transfers, the receiving federal institution should have an independent duty to establish the legality, necessity, proportionality, source, accuracy, context, retention rules, and onward-disclosure limits for its own collection and use. A federal institution should not be able to assume information is lawfully usable merely because another public body was willing or permitted to disclose it.

3. Do you agree that designating official sources for certain types of personal data would help facilitate faster and efficient services across government programs and to Canadians? (See proposal 2)

Neither agree nor disagree

While it is true that official sources may improve accuracy in some contexts, errors in an official source can spread across programs and become harder for people to identify, correct, and contest.

Official sources risk creating national-identifier infrastructure and whole-of-government data linkage. The *Act* should prohibit universal identifiers and cross-program identifiers unless Parliament expressly authorizes them and builds in strict purpose limits, rights to access and correct personal information, independent oversight empowered to make binding and enforceable decisions, and sunset/review requirements.

Any designation of an official source should require, before coming into force: public notice of the intended designation in plain language; privacy impact, human-rights, and equality assessments; retention limits for personal data; audit trails for access to personal data in the official source; and correction mechanisms that are accessible to the public. High-risk designations should additionally be subject to Privacy Commissioner review in advance of the designation becoming operational.

All designated official sources of personal data should be restricted from policing, immigration, national-security, benefit-compliance, or predictive analytics use unless specifically authorized by rights-protective primary legislation. Information disclosure for these purposes is too consequential to bypass the full scrutiny of the ordinary

legislative process in favour of a more limited regulation-making process.

Where an "official source" feeds multiple jurisdictions or programs, the *Act* must require correction propagation: correcting the source record must also correct copies, derived records, risk scores, flags, and onward disclosures held by recipients.

Theme 2: Enhancing accountability and transparency

4. Do you agree with the approach overall?

Somewhat agree

We support statutory PIAs, public access to PIAs or meaningful summaries, stronger notices, a more useful registry, and rights related to automated decision systems. The proposals should be broadened so accountability applies before harm occurs, not only after decisions are made.

PIAs should be required for all programs, technologies, data sharing, data matching, vendor processing, law-enforcement tools, biometrics, genetic collection/analysis, open-source intelligence, and uses of publicly available or commercially obtained data. The registry should disclose data-sharing agreements, PIAs, ADS records, retention schedules, breach summaries, audits, corrective-action plans, vendor/contractor arrangements, and exemptions invoked.

Accountability must also cover interjurisdictional information lifecycles. A person should not have to determine which institution collected, disclosed, received, used, retained, further disclosed, or destroyed information before knowing which privacy commissioner can help. The *Act* should require joint PIAs, shared audit records, and coordinated oversight where federal institutions participate in recurrent or high-risk transfers with other public bodies.

Accountability must also cover public-private surveillance pipelines. Evidence from land-defence and environmental protest contexts shows why *Privacy Act* modernization must address personal information collected by private security,

corporate contractors, and private intelligence vendors when they operate alongside, for, or in ways that influence public institutions. In the Tiny House Warriors context, BCCLA reported 24/7 filming by unidentified men in unmarked vehicles, a TMX robotic surveillance tower pointed at the village and into a private tiny house, cameras installed on public land with no notice identifying the collector or purpose, and workers with hardhat cameras who refused to identify who they worked for or why they were collecting personal information.

The UN Committee on the Elimination of Racial Discrimination subsequently wrote to Canada that information before it alleged escalating force, surveillance, and criminalization of Secwepemc and Wet'suwet'en land defenders by the RCMP, CIRG, and private security firms, specifically naming the Tiny House Warriors as targets of surveillance and intimidation. These examples demonstrate a serious transparency gap: affected people may not know whether surveillance is being conducted by a public body, Crown corporation, private security contractor, or some combination of them; what legal authority applies; whether the information is retained; and whether it is shared with police, regulators, prosecutors, or private companies.

The same concern appears in other public records and reporting. In the Wet'suwet'en/Coastal GasLink context, The Guardian reported close RCMP–CGL operational coordination, including police attendance at company planning sessions and daily "tailgate" meetings, while CGL retained private security firms that tracked Indigenous people's movements. The Narwhal reported that private security sat outside Gidimt'en camp 24/7 filming people walking or driving on the road, and that Wet'suwet'en community members sued the RCMP, Coastal GasLink, and Forsythe Security, while noting those allegations were denied and unproven. APTN reported a concrete information-flow concern: a C-IRG officer's affidavit relied on a CGL incident report written by a Forsythe Security employee. These examples support a *Privacy Act* rule that federal institutions must not obtain, rely on, or operationalize personal information from private actors unless the institution can document the lawful authority, necessity, proportionality, source, collection method, retention period, sharing history, and safeguards.

A modernized *Privacy Act* should also address public bodies' use of private

surveillance and intelligence vendors. At Fairy Creek, reporting based on access-to-information records indicated that the RCMP's C-IRG paid a private intelligence company for an "online intelligence report" on protest activity. More broadly, the Privacy Commissioner's Project Wide Awake report found that the RCMP used private-sector surveillance and monitoring services to collect personal information from social media, forums, the dark web, location-based services, and fee-for-access databases, and that the RCMP had not taken necessary steps to ensure service-provider collection practices complied with Canadian privacy law. The *Act* should therefore require public registries of vendor-assisted surveillance tools, mandatory privacy impact assessments before deployment, proactive publication of plain-language PIA summaries, auditable records of all disclosures from private actors to public institutions, and enforceable rules preventing government institutions from indirectly collecting personal information through private actors where the institution could not lawfully collect it directly.

5. Do you agree that Privacy Impact Assessments should be elevated to a legal requirement for government programs and activities that use personal data to make decisions that directly impact individuals? (See proposal 3)

   Agree

Yes. PIAs should be legally required where personal data is used to make or support decisions that directly affect people.

However, that trigger is too narrow. Privacy harms arise from surveillance, collection, linkage, retention, data matching, vendor processing, disclosure to law enforcement or intelligence agencies, biometric or genetic collection, open-source intelligence, and chilling effects even when no formal decision is made.

The *Act* should require PIAs before implementation for all new or substantially changed programs, activities, projects, systems, technologies, data-sharing arrangements, automated systems, biometric tools, policing/border/intelligence tools, public-private partnerships, cross-border processing, and uses of publicly available or

commercially obtained data.

Existing programs and technologies should not be grandfathered. Existing PIAs should be published, and new legally compliant PIAs should be completed and published on a prescribed schedule.

PIAs should be mandatory for recurrent, systematic, bulk, integrated-system, data-matching, or program-level information exchanges between federal institutions and provincial, territorial, municipal, Indigenous, educational, policing, health, transportation, or social-service bodies. The PIA should assess the complete exchange: collection, disclosure, receipt, use, onward disclosure, retention, correction, deletion, and remedies.

6. Do you agree that publishing plain-language summaries of Privacy Impact Assessments, subject to national security, law enforcement, and confidentiality limitations, would improve public understanding of privacy risks and safeguards? (See proposal 3)

Somewhat agree

Public bodies should publish a current, searchable PIA register and should publish each completed PIA in full, or at minimum a meaningful public summary, before or soon after launching a system, project, program, or activity involving personal information.

BCCLA's position is that full PIAs are preferable. If the government proceeds with summaries, summaries must identify the legal authority, purpose, data categories, affected groups, recipients, vendors/contractors, retention periods, automated tools, risks, mitigation measures, complaint routes, and a meaningful summary of Privacy Commissioner comments.

Public bodies, or a central PIA repository, must publish a current, searchable PIA register and must publish each completed PIA, in addition to a meaningful plain-language public summary, before or soon after launching a system, project, program, or activity involving personal information. Redactions may be made only under specified

grounds such as personal privacy, cybersecurity, legal privilege, and genuine third-party confidential information. Public-body-authored PIAs and summaries should be reusable under an open government licence.

Publishing PIAs would reduce duplicative access to Information processing, improve public trust, give public bodies one authoritative version of the PIA to maintain, and let the public, researchers, journalists, and affected communities understand privacy risks without each filing separate access requests.

Exceptions for national security, law enforcement, and confidentiality should be narrow, specific, evidence-based, time-limited, and require approval by an independent oversight agency before they can be used by the public body to withhold that portion of the PIA. The oversight bodies provided with the legal authority can be distinct according to the exception invoked (e.g., the National Security Intelligence and Review Agency could approve redactions about national security, the Civilian Review and Complaints Commission could approve redactions about law enforcement, and the law could allow or require these bodies to consult with the Privacy Commissioner in making their approval decisions). BCCLA has seen these exceptions invoked many times without justification under privacy and access legal frameworks, and it takes substantial resources (including time) and sophisticated knowledge to persevere in challenging them. The challenge process can take years before the improper redactions are ordered to be removed, years during which access is denied without merit.

Full PIAs should always be filed with the Privacy Commissioner, even where public PIAs or summaries are partly redacted.

For interjurisdictional arrangements, the PIA or their public summary should explain what information is shared, between which institutions, for what purposes, under what authority, for how long, what onward disclosures are allowed, and how an individual may obtain transfer-history information or complain.

7. Do you agree that replacing Personal Information Banks (PIBs) and classes of personal information with a single, centralized registry of personal data holdings

would improve transparency for individuals seeking to understand how their data is used? (See proposal 4)

Somewhat agree

A centralized registry could improve transparency only if it is more user-friendly, navigable, timely, plain-language, and complete than the current PIB system.

The registry should disclose legal authority, purposes, data categories, affected groups, retention periods, data-sharing agreements, PIAs, ADS records, vendor/contractor arrangements, breach summaries, audits, corrective-action plans, and exemptions relied upon.

The registry is not a replacement for access rights. It should improve access-request routing, help requesters identify where their data is held, and make systemic information visible without requiring individual access requests.

The registry should include recurrent interjurisdictional transfers and information-sharing agreements. It should identify the source institution, receiving institution, frequency of disclosure, categories of affected people, retention/destruction rules, onward-disclosure limits, audit obligations, complaint routes, and every oversight body with jurisdiction.

Individuals should have a right to obtain a transfer history of their personal information, subject only to specific, injury-based, time-limited exceptions. This is essential where information may move from a school, transit authority, health body, municipal body, provincial ministry, private contractor, or police partner to the RCMP or another federal institution.

The registry should also identify vendor-assisted surveillance, private-security information flows, and any federal reliance on information collected by private actors.

8. Do you agree that, upon request, institutions should be required to provide individuals a general explanation of how an automated decision system made or

supported a decision about them and to describe the data that was used in making or supporting that decision? (See proposal 5)

Somewhat agree

Explanations should be sufficiently detailed and specific for an individual to decide whether to seek judicial review, correction, reconsideration, or another remedy.

The explanation should identify the system used, the role of automation, the data and factors relied upon, the source of the data, known limitations, how to correct source data, and how to seek human review by a person with authority to change the outcome. There should be statutory deadlines calibrated so requesters can obtain advice and decide whether to challenge a decision before limitation periods expire, with meaningful consequences for late or inadequate explanations.

The same or analogous requirements should apply to ADS used for systemic decisions or decisions that indirectly affect people, including testing for accuracy and bias before deployment and monitoring outcomes for human-rights compliance.
Where an ADS relies on data received from another jurisdiction or a private actor, the explanation should disclose that source and any transfer history needed to understand whether inaccurate, incomplete, or context-stripped information influenced the outcome.

9. Do you agree that institutions should be required to notify individuals when their personal data is used by automated decision systems to make or influence decisions about them? (See proposal 6)

Somewhat agree

Notice should be required, but it should generally be provided before the system uses the individual's data or before the decision is made, so the person can meaningfully contest the use or seek a remedy.

Notice after the system starts using personal data is inadequate where the purpose is to prevent harm, not merely explain it after the fact.

The notice should identify the system, purpose, legal authority, data categories, data sources, role of human decision-makers, appeal routes, correction rights, and how to request a meaningful explanation.

If the data came from another public body, private contractor, data broker, security firm, or foreign/vendor processor, the notice should identify that source unless a specific, injury-based, time-limited exception applies.

10. Do you agree that institutions should be required to provide privacy notices in plain language, make them available as soon as reasonably possible when personal data is collected, and publish them in a centralized register of personal data holdings? (See proposal 6)

Agree

Privacy notices should be plain language, accessible, timely, and published in a centralized location whether or not that location is called a register of personal data holdings.

"As soon as reasonably possible" should generally mean at or before collection. Delayed notice should require a documented reason and independent review where delay is based on law enforcement, national security, or safety.

Notices should explain legal authority, purpose, mandatory/optional status, consequences of refusal, recipients, retention, complaint routes, automated processing, and access/correction rights.

The *Act* should address indirect collection. When a federal institution collects personal information from another public body, private actor, or foreign/vendor processor, individuals should be told what information was collected, when, from whom, in what circumstances, for what purpose, and how long any notice delay will last. Delayed

notice should be reviewed at prescribed intervals and provided once the risk has ended.

Safe-access protections should be considered for education, transportation, health, victim, housing, immigration, and social-service contexts so that information given to obtain essential services is not quietly repurposed for unrelated enforcement unless strict statutory conditions are met.

Theme 3: Advancing safeguards across the spectrum of data sensitivity

11. Do you agree with the approach overall?

Somewhat agree

The approach moves in the right direction by addressing sensitivity, identifiability, breach management, safeguards, necessity for collection, disposal, and retention. Sensitivity should be contextual and include metadata, location patterns, biometrics, images, voice, device identifiers, behavioural traces, inferences, risk scores, genetic information, and group/community impacts.

Necessity, proportionality, effectiveness, and least-intrusive-means duties should apply across the full lifecycle: collection, creation, inference, linkage, use, disclosure, sharing, automated processing, retention, and disposal.

The lifecycle must include interjurisdictional movement of data. Safeguards should not stop when information crosses a federal-provincial, federal-municipal, school-police, health-police, transit-immigration, or public-private boundary.

12. Do you agree that explicitly recognizing in law a spectrum of data sensitivity and identifiability, from anonymized to highly sensitive personal data, improves clarity and supports more consistent privacy protection? (See proposal 7)

Agree

Yes. The *Act* should recognize that identifiability and sensitivity exist on a spectrum and depend on context.

Information sensitivity should be assessed based on the highest foreseeable harm in context. For example, information about sexual orientation may be much more sensitive for a closeted person than for someone who is publicly out.

The *Act* should include direct identifiers, quasi-identifiers, metadata, location patterns, biometrics, images, voice, genetic information, behavioural traces, linked datasets, inferences, labels, profiles, risk scores, and automated predictions.

Genetic information should be treated as highly sensitive because it can identify a person, reveal familial relationships, affect relatives who never interacted with police, and remain useful for future searches or kinship analysis.

Information about participation in protests, land defence, Indigenous governance, border interactions, schools, shelters, health care, transit, or other essential-service contexts should be treated as sensitive because disclosure or function creep may deter people from exercising rights or accessing services.

13. Do you agree that creating legal requirements for breach management, notification and reporting improves the protection of personal data? (See proposal 8)

Agree

Yes. Mandatory breach management, notification, and reporting are essential public-sector privacy duties.

Individuals affected by an improperly managed breach should have access to meaningful remedies.

Materiality should be assessed solely by risk to affected individuals, including bodily harm, humiliation, damage to reputation or relationships, loss of employment or

opportunities, financial loss, identity theft, negative credit effects, property damage, immigration/enforcement consequences, or risks to safety.

Institutions should keep breach logs, conduct root-cause analysis, implement corrective measures, and publish aggregate reports.

Where breached information has been shared across jurisdictions or with vendors, the institution should notify all recipients, require containment and deletion/correction steps, and provide affected people with a clear explanation of the full transfer chain.

14. Do you agree that requiring institutions to use physical, technical, and administrative security measures that are proportionate to the sensitivity of the personal data is appropriate? (See proposal 9)

Agree

Yes. Security safeguards should be mandatory, enforceable, and proportionate to sensitivity, identifiability, volume, context, and foreseeable harm.

Safeguards should include access controls, encryption, logging, staff training, vendor due diligence, privacy-by-design, threat modelling, retention controls, independent testing, and incident response.

Heightened safeguards should apply to policing, border, intelligence, immigration, benefits, health, children's data, Indigenous data, biometrics, genetic information, location data, and automated decision systems.

For interjurisdictional exchanges, safeguards must include common security standards, audit logs, source notation, correction propagation, retention/destruction rules, and restrictions on onward disclosure by every participant in the chain.

15. Do you agree with the proposed criteria for limiting the collection of personal data to what is demonstrably necessary, effective, minimally intrusive, and directly related to a program or activity? (See proposal 10)

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

Somewhat agree

Yes. The proposed criteria are core safeguards and should be included in the *Act*. The collection of personal data should also be proportionate, considering sensitivity, the risk that a breach or misuse would create for an individual or group, and the importance of the program objective.

Analysis of necessity, effectiveness, minimal intrusiveness, proportionality, and direct relationship should be documented before or at the time of collection for monitoring, audit, administrative review, and judicial review.

These criteria should apply not only to collection but also to creation, inference, linkage, use, disclosure, sharing, automated processing, retention, reliance on publicly available data, and procurement of third-party services.

For information received from another jurisdiction or private actor, the federal institution should assess the source, accuracy, reliability, context, legal authority, and whether the information was originally collected for an essential-service purpose that should not be repurposed for enforcement.

Covert DNA collection through items such as tea cups shows why "collection" must include indirect, surreptitious, or vendor-assisted collection of genetic information. The *Act* should require explicit lawful authority, necessity, proportionality, judicial authorization or informed consent for surreptitious genetic collection, and audit records showing what was collected, tested, retained, destroyed, or shared.

16. Do you agree that institutions should be legally required to dispose of personal data that was collected inadvertently? (See proposal 11)

Agree

Yes. Maintaining inadvertently collected personal information risks unnecessary privacy breaches and function creep.

Records should document the sensitivity of the information, how collection occurred, steps taken to securely dispose of it, and whether any recipient must also delete or return copies.

The core obligation should be in the *Act*, while detailed compliance procedures can be prescribed by regulation.

There should be narrow exceptions to preserve records needed for an investigation, complaint, legal proceeding, audit, or accountability review, but the information should be segregated, access-restricted, and not used operationally.

Disposal duties should include auditable destruction records and should address derived information, copies, genetic profiles, vendor-held data, and information shared onward across jurisdictions or with private contractors.

17. Do you agree that that there should be a legal requirement for institutions to limit their retention of personal data to only that which is necessary for the operating program or activity? (See proposal 11)

Agree

Yes. Retention limits should be legally binding and tied to the specific authorized purpose.

Maintaining unnecessary information risks privacy breaches, function creep, future profiling, and reliance on stale or inaccurate data.

Records should confirm the method and timing of secure disposal and should document how the information came into the institution's possession so that unnecessary information-sharing pipelines can be identified and shut down.

Retention schedules should be public in the registry and justified in PIAs. Retention limits should follow the information across recipients. If information is corrected, deleted, or found unlawfully collected, the institution should notify every

recipient and require deletion, return, correction, or restricted use of all copies and derived information.

Theme 4: Modernizing foundation for privacy and trust

18. Do you agree with the approach overall?

Somewhat agree

We support recognizing privacy as a fundamental right, incorporating privacy principles, adding modern definitions, and addressing Indigenous rights regarding data.

The purpose clause should make privacy, dignity, autonomy, equality, democratic participation, freedom of expression and association, Indigenous rights, and the rule of law operative legal guides, not preambular aspirations.

"Enabling service" should not dilute rights. Service improvement must occur within rights-protective limits.

Privacy principles should be enforceable duties with clear burdens, records, disclosure obligations, audits, and remedies.

The *Act* should state that privacy protections follow the information and the person across institutional, jurisdictional, and public-private boundaries. A person should not lose practical access to privacy rights because their data crossed an invisible legal boundary.

19. Do you agree that the *Privacy Act* should be amended to recognize privacy as a fundamental right, emphasize the importance of enabling service, and advance reconciliation with Indigenous peoples? (See proposal 12)

Somewhat agree

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

We strongly support recognizing privacy as a fundamental right and core democratic value.

Recognition must be enforceable. The *Act* should require all federal powers and exceptions to be interpreted consistently with privacy, dignity, autonomy, equality, freedom of expression and association, Indigenous rights, and the *Charter*.

"Enabling service" should be secondary to rights. Administrative efficiency, cost savings, convenience, and speculative future use should not justify intrusive data practices.

Reconciliation-related provisions must be co-developed with Indigenous governments, organizations, rights holders, and Indigenous data-governance experts. Different models may be most appropriate for different Indigenous Nations.

The *Act* should protect Indigenous self-determination, Indigenous data sovereignty, collective as well as individual interests, and distinctions-based governance. Recognizing privacy as a fundamental right should also require "safe access" protections so people are not deterred from schools, health care, transit, housing, victim services, social supports, or other essential services because information may be redirected to unrelated enforcement systems.

20. Do you agree that listing the proposed privacy principles and incorporating them into the *Privacy Act* requirements would help strengthen practices and make the rules easier to interpret and apply? (See proposal 13)

Somewhat agree

The "other principles" listed in Proposal 13 — privacy by design, necessity, proportionality, effectiveness, and minimal intrusiveness — reflect constitutional considerations when s. 8 of the *Charter* is implicated and must be included.

British Columbia Civil Liberties Association
306 – 268 Keefer Street
Vancouver. BC, Canada V6A1X5
Tel 604.687.2919
Fax 604.687.3045
Toll-free 1.855.556.3566
info@bccla.org
www.bccla.org

These principles should apply to collection, creation, inference, linkage, use, disclosure, sharing, automated processing, retention, and disposal.

This would harmonize public bodies' understanding of privacy across contexts where s. 8 formally applies and where it may not, creating one clear framework for decision-making consistent with a free and democratic society.

Principles should not be merely interpretive. They must be enforceable statutory duties. The *Act* should add an end-to-end accountability principle: every institution participating in an information exchange is independently responsible for the lawfulness, necessity, accuracy, security, retention, correction, deletion, and onward disclosure of the information it receives or discloses. Authorization by one institution should not relieve another institution of its obligations.

21. Do you agree that adding definitions for key concepts such as privacy breach, material breach, publicly available personal data, sensitive data, creation of personal data, inadvertent collection, anonymization, de-identified data and automated decision system improves legal clarity? (See proposal 14)

Agree

These definitions — particularly "material breach," "sensitive data," "publicly available personal data," "creation of personal data," "anonymization," "de-identified data," and "automated decision system" — are essential to legal clarity.

"Sensitive data" should include context-sensitive information and high-risk categories such as biometrics, location data, children's information, immigration status, health, etc.

"Publicly available personal data" must be narrow. Online visibility or commercial availability should not authorize government scraping, linking, profiling, retaining, or sharing without legal authority and necessity/proportionality analysis.

22. Do you agree that incorporating requests for personal data into the *Access to Information Act* simplifies the access regime? (See proposal 15)

Somewhat agree

The access regime is user-unfriendly and often unresponsive. Streamlining and improving user experience, especially for lay requesters, is welcome.

Consolidation may help only if it preserves and strengthens personal access, correction, and accountability rights.

An impactful reform would be a one-window access office where requests can be sent, rather than requiring individuals to know which body holds the information they seek. The regime should track response times, common request types, barriers to access, and whether requests involve information held by multiple bodies.

For interjurisdictional exchanges, individuals should not have to file separate requests with each institution to reconstruct what happened. The *Act* should create a right to a transfer history showing which institution collected, disclosed, received, used, retained, further disclosed, or destroyed their information, subject only to specific, injury-based, time-limited exceptions.

Theme 5: Indigenous Peoples' access to, and protection of, their data

23. Do you agree with the approach overall?

Neither agree nor disagree

BCCLA does not purport to answer for Indigenous governments, organizations, communities, or rights holders without consultation.

In principle, it is important that the *Privacy Act* address Indigenous data sovereignty, Indigenous self-determination, collective and individual interests, and distinctions-based governance.

Indigenous peoples' rights are inherent and must be respected consistently with s. 35 of the *Constitution Act*, 1982, UNDRIP, and Canada's UNDRIP legislation.

Federal privacy reform should not unilaterally define Indigenous data governance. Interjurisdictional information-sharing rules must be co-developed with Indigenous governments and rights holders where Indigenous data is involved. Indigenous data should not be transferred between federal, provincial, territorial, municipal, policing, child-welfare, health, education, or private bodies in ways that undermine Indigenous self-determination, safety, or data sovereignty.

24. Do you agree that the terms proposed to replace "aboriginal governments", "Indian band," and the lists of indigenous governments are appropriate? (See proposal 16)

Neither agree nor disagree

The federal government should not unilaterally decide these terms through a privacy modernization exercise.

The *Act* should avoid outdated colonial terminology and should use respectful, current, distinctions-based language that reflects Indigenous peoples' interests and governance structures.

Definitions used for interjurisdictional information sharing must not exclude Indigenous governance bodies or force Indigenous data relationships into federal categories that do not reflect Indigenous law or governance.

25. Do you agree that creating a specific category of Indigenous personal data that would be subject to distinct governance considerations is appropriate? (See proposal 17)

Neither agree nor disagree

Potentially, but only if co-developed with Indigenous governments, organizations, rights holders, and Indigenous data-governance experts.

A distinct category may help recognize collective interests, Indigenous data sovereignty, kinship and citizenship information, community protocols, and the special risks created by colonial state data systems.

The category must not become a new label that enables surveillance, profiling, policing, immigration enforcement, child welfare intervention, benefit-compliance analytics, or service denial.

The *Act* should respect distinctions-based approaches and avoid treating all Indigenous data governance issues as identical.
Distinct governance rules should follow Indigenous data through every transfer, including disclosure to or from provincial, territorial, municipal, policing, child-welfare, health, education, or private bodies.

26. Do you agree that allowing Indigenous governments to regularly receive copies of personal data through formal agreements supports Indigenous data sovereignty? (See proposal 18)

Neither agree nor disagree

Potentially, but only if co-developed with Indigenous governments, organizations, Indigenous rights holders, and Indigenous data-governance experts.

Control of a copy is not the same as control of the data. OCAP and other Indigenous data-governance principles may require more than access to copies.

Formal agreements should be distinctions-based and address purpose, consent/safety, access, correction, retention, deletion, onward sharing, audit rights, and remedies.

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

Theme 6: Updating the compliance framework

27. Do you agree with the approach overall?

Somewhat agree

We support the direction of strengthening compliance, but the proposals do not go far enough.

Corrective-action plans, information sharing between oversight bodies, re-identification offences, expanded Federal Court authority, and five-year reviews are useful but incomplete.

The Privacy Commissioner should have full binding order-making powers across the *Act*, not only authority tied to corrective-action plans.

Compliance must include collection, use, disclosure, retention, correction, destruction, safeguards, notice, PIAs, registries, information-sharing agreements, vendor processing, and automated systems.

The compliance framework must address fragmented jurisdiction. Privacy harms often cross federal, provincial, territorial, municipal, police, health, school, transportation, Indigenous, private-contractor, foreign or vendor boundaries; remedies should be coordinated and end-to-end.

28. Do you agree that granting the Privacy Commissioner binding order-making powers to require institutions to develop and publish Corrective Action Plans would strengthen compliance with the *Privacy Act* and improve accountability? (See proposal 19)

Somewhat agree

Yes, this would strengthen compliance, but it is too limited if framed only as authority to require Corrective Action Plans.

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

The Commissioner must have full binding order-making powers across the *Act*.

Orders should be able to require an institution to stop unlawful practices, delete unlawfully retained data, provide access, correct records, publish notices, redo PIAs, suspend high-risk systems, amend data-sharing agreements, implement safeguards, and report publicly on compliance.

Corrective Action Plans should be public by default, specific, time-bound, enforceable, and subject to follow-up audits.

Order-making powers should include the ability to preserve records required for an investigation; require deletion, return, correction, or restricted use of unlawfully obtained information; notify every recipient of corrected or deleted information; and suspend or terminate unlawful interjurisdictional or public-private sharing arrangements.

29. Do you agree that authorizing the Commissioner to share information with other oversight bodies, where appropriate, supports effective enforcement? (See proposal 20)

Agree

Yes. Modern privacy harms often cross institutional and jurisdictional boundaries, including public-private boundaries created by outsourcing security, surveillance, analytics, and intelligence work.

The Commissioner should be able to coordinate with information commissioners, human-rights bodies, police and CBSA oversight bodies, election regulators, procurement auditors, Indigenous governance bodies where appropriate, provincial/territorial privacy commissioners, and oversight bodies with mandates over private security, private investigators, private police, and similar actors.

Information sharing should support joint investigations, consistent remedies, systemic audits, and public-interest reporting, with safeguards for complainants, whistleblowers,

confidential sources, solicitor-client privilege, and sensitive personal information. Information sharing alone is not enough. The Commissioner must be able to use relevant legal powers to correct wrongdoing and publish findings about privacy-related impacts.

The *Act* should create a one-window complaint mechanism for interjurisdictional transfers. A complaint filed with one competent commissioner should be deemed filed, on the same date, with every other commissioner having jurisdiction, and should suspend all limitation periods.

Commissioners should be empowered to refer and transfer complaints, designate a lead commissioner, conduct joint or parallel investigations, share evidence and legal analysis, use a common evidentiary record, coordinate timelines and communications, issue complementary orders, and publish joint findings and systemic recommendations.

Consequential amendments and federal-provincial-territorial agreements will be needed so cooperation is not one-sided or asymmetrical. The modernized *Act* should create an operational joint-investigation and coordinated-remedy framework, not merely discretionary information sharing.

30. Do you agree that introducing offences for unauthorized attempts to re-identify de-identified data is appropriate? (See proposal 21)

Somewhat agree

• A re-identification offence may be appropriate for malicious, reckless, or unauthorized attempts to identify individuals from de-identified data.
• The offence should require a clear mental element and should be targeted to harmful conduct, not accidental discovery or responsible testing.
• The *Act* should protect good-faith privacy research, security testing, journalism, whistleblowing, legal advocacy, academic work, and complaints to regulators through public-interest and responsible-disclosure defences.
• Institutions should not rely on the offence as a substitute for robust anonymization standards, de-identification governance, data minimization, security safeguards, and

limits on linkage.
• The offence should also address re-identification by government institutions and recipients in interjurisdictional or vendor arrangements. Public bodies should not attempt to re-identify de-identified data unless expressly authorized by law and necessary/proportionate for a legitimate public purpose.

31. Do you agree that expanding Federal Court authority to address violations of the *Privacy Act* beyond access requests strengthens the protection of personal data? (See proposal 22)

Agree

Recourse to the courts is vital to ensure compliance and meaningful remedies when the state violates privacy rights.

Federal Court authority should extend to collection, use, disclosure, retention, safeguards, accuracy, notice, correction, destruction, PIAs, registry duties, information-sharing agreements, and automated systems.

Available remedies should include declarations, injunctions, correction and deletion orders, preservation orders, damages where appropriate, and any other just and appropriate relief.

Any alternative process must provide meaningful redress and comply with natural justice, including an opportunity to make representations.

Federal Court remedies should expressly cover interjurisdictional transfers, including unlawful receipt from another public body, unlawful onward disclosure, failure to maintain transfer-history records, failure to propagate correction or deletion, and failure to preserve records needed for a complaint or investigation.

32. Do you agree that introducing a mandatory five-year review of the *Privacy Act*, led by the President of the Treasury Board, helps ensure the legislation remains current? (See proposal 23)

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

Agree

Yes. A five-year review is necessary because data practices, AI systems, surveillance tools, and public-private data infrastructure evolve quickly.

The review should include public consultation, Indigenous co-development where Indigenous data is affected, expert evidence, civil-society participation, and independent reporting on implementation.

Treasury Board should publish annual implementation reports before each five-year review, including all published PIAs and PIAs under development, registry compliance, breaches, Commissioner orders, data-sharing agreements, automated systems, exemptions invoked, and corrective actions.

Reviews should be led transparently and should not be controlled solely by the same central agency responsible for government data policy.

Five-year reviews should evaluate whether interjurisdictional agreements, public-private surveillance arrangements, genetic-information practices, foreign/vendor processing, safe-access protections, and joint-oversight mechanisms are working and whether sunsetted high-risk programs should be re-authorized.

33. Do you agree that, taken together, the proposed changes represent a clear and coherent modernization of the *Privacy Act*?

Somewhat agree

The proposals contain important building blocks, but they are not yet a coherent rights-protective modernization.

The strongest elements are recognition of privacy as a fundamental right, necessity for collection, PIAs, breach duties, safeguards, ADS notice/explanation, registry reform, Indigenous data attention, and expanded compliance tools.

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

The central weakness is that broad data-sharing and reuse powers appear before sufficiently strong legal limits, independent oversight, public transparency, and remedies.

The *Act* should not treat personal data as a reusable government asset. It should set strict public-law conditions for collection, creation, inference, linkage, sharing, automation, retention, and disclosure.

The proposal is not coherent unless it addresses end-to-end accountability for interjurisdictional transfers, public-private surveillance pipelines, genetic privacy, foreign/vendor processing, safe access to essential services, correction propagation, transfer-history rights, and coordinated remedies across regulators.

Privacy protections should follow the information and the person, not stop at the boundary of a federal institution. The modernized *Act* should expressly regulate federal participation in interjurisdictional information exchanges with provincial, territorial, municipal, Indigenous, educational, policing, health, transportation, immigration, social-service, and other public bodies.

Federal institutions should participate in such transfers only where the transfer serves a specific lawful purpose, is necessary and proportionate, uses the minimum information required, cannot be achieved by a less intrusive means, accounts for source accuracy and context, and is subject to retention, access, security, correction, deletion, onward-disclosure, audit, and independent oversight rules.

Recurrent, systematic, bulk, integrated-system, data-matching, or program-level exchanges should require written information-sharing agreements, PIAs, public registry entries, transfer-history rights, fixed expiry dates, and mandatory periodic review.

Agreements should identify legal authority, responsible officials, affected groups, categories of information, disclosure frequency, accuracy controls, correction propagation, audit logs, breach procedures, complaint routes, suspension/termination procedures, and oversight rights.

British Columbia Civil Liberties Association
306 – 268 Keefer Street
Vancouver. BC, Canada V6A1X5
Tel 604.687.2919
Fax 604.687.3045
Toll-free 1.855.556.3566
info@bccla.org
www.bccla.org

BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION

The *Act* should create a one-window complaint mechanism. A complaint about an interjurisdictional transfer filed with one competent commissioner should be deemed filed with every commissioner having jurisdiction. Commissioners should be able to coordinate investigations, share evidence, issue complementary orders, and publish joint findings.

Safe-access protections are needed for children, newcomers, people with precarious immigration status, victims or witnesses, people in mental-health crisis, and people seeking education, transit, health care, housing, social services, or safety. Information collected to provide essential services should not be redirected to unrelated enforcement unless strict statutory conditions are met.

The *Privacy Act* should also expressly cover personal information collected, created, inferred, or supplied by private security firms, contractors, Crown-corporation agents, private investigators, data brokers, intelligence vendors, laboratories, and technology providers when that information is collected for, shared with, relied on by, or used to influence a federal institution. Reports concerning Tiny House Warriors, Wet'suwet'en land defenders, Fairy Creek, and RCMP vendor-assisted intelligence show why this is necessary.

Genetic information requires special protection. The reported tea-cup DNA collection in the Ibrahim Ali investigation shows that people may not know whether their DNA was collected through *Privacy Act* indirect collection rules; whether samples or profiles remain held; or whether information was shared with laboratories, foreign entities, or other bodies. The *Act* require explicit lawful authority, necessity/proportionality analysis, judicial authorization or informed consent for surreptitious genetic collection, strict vendor/foreign processing limits, audit trails, and destruction/notification rights for people not subject to lawful criminal investigation with requisite authorizations.

Without these measures, information collected in one context can cross a jurisdictional or public-private boundary, acquire a new purpose, and produce serious consequences without timely notice or a practical means of obtaining a complete explanation or remedy. That is incompatible with meaningful privacy protection, democratic accountability, and the rule of law.

British Columbia Civil Liberties Association
306 – 268 Keefer Street
Vancouver. BC, Canada V6A1X5
Tel 604.687.2919
Fax 604.687.3045
Toll-free 1.855.556.3566
info@bccla.org
www.bccla.org