

WHiSSPR Report: Bill C-36 Assessment (2026)

Mark Lizar

WHiSSPR Report: Bill C-36 Assessment (2026)

White Hat Identity, Surveillance, Security, Privacy and Risk (WHiSSPR) Report Full Title:
Assessing Governance Capacities of Bill C-36, the Protecting Privacy and Consumer Data
Act Author: Mark Lizar Published by: Global Privacy Rights Lab: Transparency Lab
Published: 2026 License: Global Privacy Rights, Copyright 2026

Source assessed: Bill C-36, 45-1, first reading text as introduced 15 June 2026, read in full.
Clause numbers are as at first reading and will move in committee.

 WHiSSPR rating method (TPI v2) defaults - Scoring orientation: ordinal categories on the ANCR TPI scale. +1 dynamic, in context. 0 present but static or out of context. -1 present but obstructed. -3 non-operable. - Indicator family: Kantara ANCR Transparency Performance Indicators (TPI). - **No composite is defined and none should be inferred.** The ratings are ordinal categories rather than measurements on a continuous scale, so arithmetic across them, including any weighted sum, does not produce a comparable figure. Annex E of the ANCR extension states this, and this report observes it. - Assurance ladder: a contract reaches level 3 when accountability behind each identifier traces to a named party under a named instrument. It reaches dynamic secure level 4 when the access itself is credentialed at the point of request, logged to a party that is not the requester, actively approved rather than standing, and bounded in time and scope.

Figures

Figure 1	The notice fork
Figure 2	What the Act records, and who is allowed to read it
Figure 3	Where the Act places notice in the identification sequence
Figure 4	The assurance ceiling and the stage profile
Figure 5	The route opened by sections 92 to 96
Figure 6	Two bills, six years, the same two clauses

About WHiSSPR Reports

A WHiSSPR Report, White Hat Identity, Surveillance, Security, Privacy and Risk, is an audit of the privacy and security of identity surveillance. The order of the letters is the method, and each stage is answered before the next is asked.

- **Identity.** Which identifiers the instrument reaches, what the actual scope of disclosure of each is when checked against permissions and exposure rather than against what is claimed, and whether any official or contractual use is named, because only a named use supports a claim of legitimate status.
- **Surveillance.** What observation the instrument permits against those identifiers. Who can see, what is emitted, what is retained, what is inferable.
- **Security, meaning the security of that surveillance.** Not whether unauthorised access occurs, but whether the authorised access is accountable.
- **Privacy risk.** The residual once the first three are known, recorded rather than resolved.

Applied to a statute rather than to a contract, the output is a ceiling and a floor: the best assurance any contract made under the Act could claim, and the worst it guarantees.

WHiSSPR uses the Kantara Initiative Data Controller Identity Record schema and Transparency Performance Indicators to assess transparency performance and measure operational accountability.

Executive Summary

Bill C-36 enacts the Protecting Privacy and Consumer Data Act and replaces the private sector provisions of PIPEDA. It was introduced on 15 June 2026 and is at second reading. It is the third federal attempt in six years, after Bill C-11 and Bill C-27, and it is materially better than either.

It is also, on the measures WHiSSPR exists to test, unchanged.

What improved

1. **Inference is in scope.** Section 2(1) defines personal information as information about an identifiable individual, **including information that is inferred about the individual.** Neither PIPEDA nor Bill C-27 said this. It is the single most consequential drafting change in the Act for artificial intelligence governance.
2. **Purposes must be recorded before collection.** Section 12(3) requires an organization to determine and record each purpose at or before the time of collection. Section 12(4) extends this to new purposes.

3. **Consent now carries a disclosure set.** Section 15(3) requires purposes, manner, foreseeable consequences, the specific type of information, and the names or types of third parties, before consent is sought.
4. **Legitimate interest is conditioned.** Section 18(4) requires the interest to be identified and described, a privacy impact assessment carried out, and mitigation applied. Section 18(5) requires the description and assessment to be recorded.
5. **Consent cannot be tied or deceived.** Sections 15(7) and 16.
6. **Codes of practice and certification programs acquire a statutory route.** Sections 92 to 96.
7. **Enforcement is real.** Section 114 sets an administrative penalty at the greater of \$10,000,000 and 3 per cent of gross global revenue. Offence provisions reach the greater of \$25,000,000 and 5 per cent.

What did not change

1. **Section 8(1) is word for word the clause assessed in the 2024 report on Bill C-27.** An organization must designate an individual and provide that individual's business contact information to any person who requests it. The finding made in 2024 stands without amendment.
2. **Section 62(1) is likewise word for word the Bill C-27 clause.** Section 62(2) adds seven required disclosures, which is a genuine improvement, and none of them is the identity of the controller.
3. **There is no requirement to identify the controller before collection.** The Act names no point at which an individual, before being identified, can learn who is accountable.
4. **There is no receipt, no proof of notice, and no record of the notice event.** The word receipt does not appear in the Act. Every record the Act creates is held by the organization and disclosed to the regulator on request.

Bill C-27

introduced 2022, died on the Order Paper

s.8(1)

An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act. It must provide the designated individual's business contact information to any person who requests it.

identical

s.62(1)

An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations under this Act.

identical

Bill C-36

introduced 15 June 2026, at second reading

s.8(1)

An organization must designate one or more individuals to be responsible for matters related to its obligations under this Act. It must provide the designated individual's business contact information to any person who requests it.

s.62(1)

An organization must make readily available, in plain language, information that explains the organization's policies and practices put in place to fulfill its obligations under this Act.

Two clauses were compared. The report does not claim the bills are otherwise identical.

The clauses are unchanged, so the 2024 assessment of them applies unchanged to Bill C-36.

Source: Bill C-27 cl.8(1), 62(1); Bill C-36 ss.8(1), 62(1). Assessment: Transparency Lab, published by Global Privacy Rights.

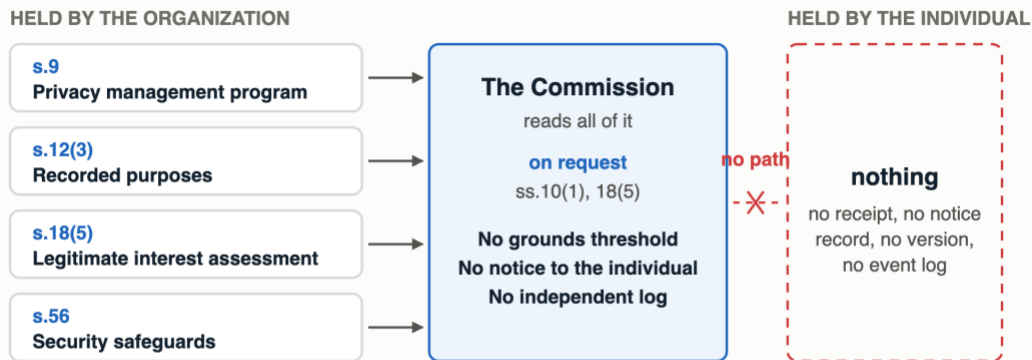
Figure 6. Two bills, six years, the same two clauses. Sections 8(1) and 62(1) appear in Bill C-36 in the words assessed in the 2024 report on Bill C-27.

Figure 6. Two bills, six years, the same two clauses. Sections 8(1) and 62(1) appear in Bill C-36 in the words assessed in the 2024 report on Bill C-27.

Conclusion

Bill C-36 builds a compliance regime with teeth and leaves the evidence problem untouched. It requires organizations to record what they do and to show those records to a regulator. It requires nothing to be shown to the individual at the moment of collection, and it produces no artefact the individual holds, meaning online consent can only be governed retroactively.

The result is a regime in which a contravention can be penalised at 3 per cent of global revenue and an individual still cannot demonstrate what they were told, or when, or by whom.



Source: Bill C-36, ss.9, 10(1), 12(3), 18(5), 56, 62. Assessment: Transparency Lab, published by Global Privacy Rights.

Figure 2. What the Act records, and who is allowed to read it. Every record the Act creates is held by the organization and disclosed to the Commission on request. The individual holds nothing.

Figure 2. What the Act records, and who is allowed to read it. Every record the Act creates is held by the organization and disclosed to the Commission on request. The individual holds nothing.

The Three Questions

1. How much notice and transparency is actually required?

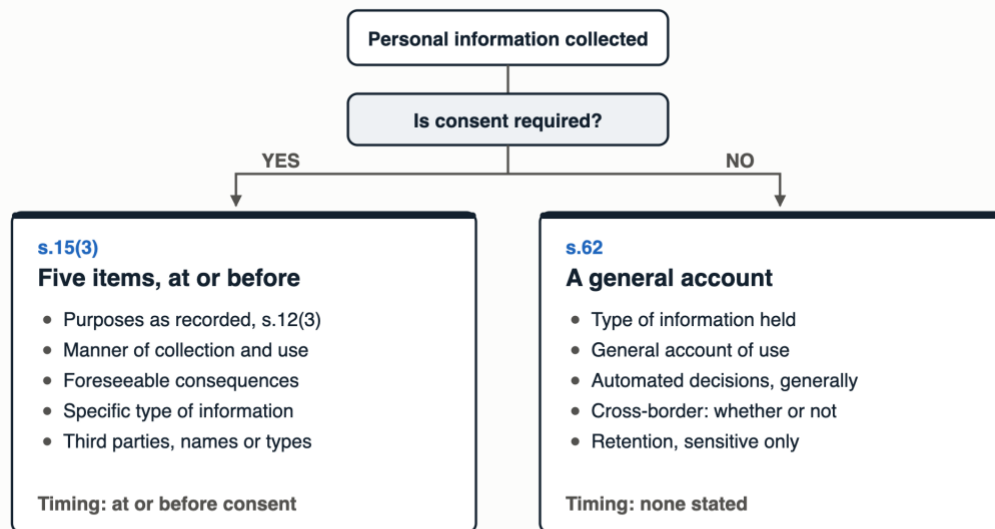
Two quanta, and which applies depends on whether consent is required at all.

Where consent is required, section 15(3) sets five items to be provided at or before the moment consent is sought: the purposes as recorded under section 12(3), the manner of collection, use or disclosure, the reasonably foreseeable consequences, the specific type of information, and the names or types of third parties. This is the strongest notice provision in Canadian federal privacy law to date.

Where consent is not required, the quantum is section 62 alone: a general account, readily available, with no timing obligation and no connection to any processing event.

The exceptions determine which quantum governs, and they are wide. Section 18(3) permits collection, use **and disclosure** under legitimate interest with no notice to the individual at any point, which is un-governed surveillance. Section 19 permits transfer to a service provider with no notice. Section 14(2) lists more than thirty provisions under which information may be used or disclosed for a purpose other than the recorded one. Making digital privacy almost impossible.

So the operative answer is this. The notice quantum is conditional, and on the pathways most processing will actually use, it collapses to an undated general account published somewhere on a website. Section 62 carries no timing, no specificity, no jurisdiction for cross-border transfers beyond a yes or no, and no version. What the Act requires to be *known* and what it requires to be *shown at the moment it matters* are different, and only the first is legislated.



ss.18(2), 18(3), 19 and 14(2) place processing on the right-hand branch.

Source: Bill C-36, ss.14, 15, 18, 19, 62. Assessment: Transparency Lab, published by Global Privacy Rights.

Figure 1. The notice fork. Where consent is required, section 15(3) sets five items at or before. Where it is not, section 62 gives an undated general account, and the exceptions decide which branch carries the traffic.

Figure 1. The notice fork. Where consent is required, section 15(3) sets five items at or before. Where it is not, section 62 gives an undated general account, and the exceptions decide which branch carries the traffic.

2. Will consent still be valid?

Legally valid on the face of the Act. Operationally unprovable.

Section 15(3) makes consent invalid unless the five items are provided. Section 16 invalidates consent obtained by deception. Section 15(7) forbids tying consent to service provision beyond what is necessary. Section 15(5) narrows implied consent, and section 15(6) forbids relying on it for section 18 activities. Each of these is a genuine improvement.

But nothing in the Act requires that the section 15(3) provision be recorded. There is no receipt, no notice record, no version, and no notice event log. The word notice or consent receipt does not appear in the Act. Transparency is not enforced.

The consequence is symmetrical in the wrong direction: an organization that complied perfectly and an organization that did not comply at all produce identical evidence, which is none. When the Commission moves to penalise under section 114 at 3 per cent of gross global revenue, it must establish what an individual was told, and the only account available is the account of the party under investigation.

Consent is valid in law and unfalsifiable in fact. That is a worse position than either a strict regime or a permissive one, because it makes the enforcement power unusable at the margin (by people) where it matters.

3. Are there privacy officers to implement the Act?

No. There is a contact point.

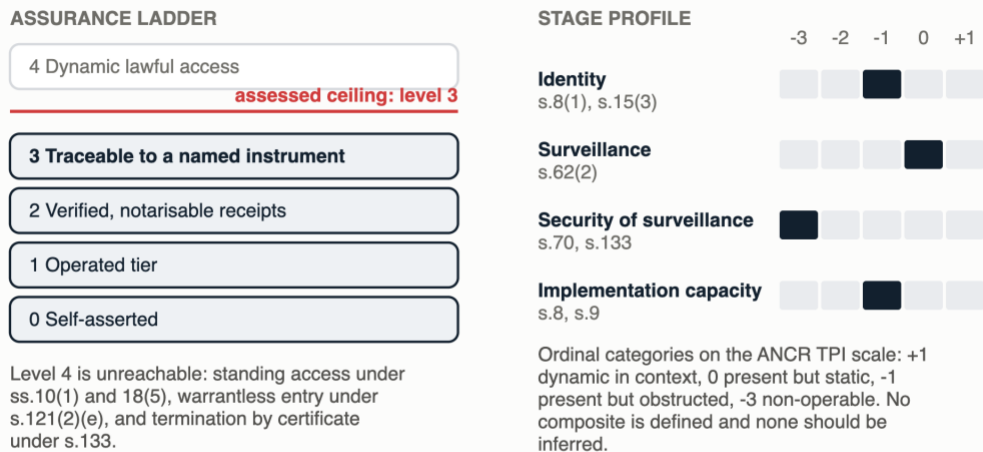
Section 8 is the whole of it, and it is two sentences. An organization must designate one or more individuals responsible for matters related to its obligations, and must provide that individual's business contact information to any person who requests it. Section 8(2) confirms the designation does not relieve the organization.

Nothing else in the Act addresses the role. There is no qualification requirement, no independence requirement, no seniority floor, no reporting line, no protection against dismissal for performing the function, no threshold that triggers the appointment, and no obligation to publish who the individual is.

Compare. Quebec Law 25 section 3.1 makes the person exercising the highest authority the person in charge by default, and requires the title and contact information to be **published on the enterprise's website**. GDPR Articles 37 to 39 require designation on defined triggers, publication of contact details, independence, a direct reporting line to the highest management level, and protection from dismissal or penalty for performing the task.

Bill C-36 has none of these. Section 9 requires a privacy management program, and section 10(1) requires it be shown to the Commission on request, but the Act does not require anyone competent, senior, independent or publicly identifiable to run it.

This is the implementation gap. The Act creates binding orders, third party audits at the organization's cost under section 119, and penalties at 3 per cent of gross global revenue, and it does not create the professional function that would let an organization meet any of it. The whistleblower protection at section 144 protects an employee who reports a contravention. Nothing protects the designated individual who tries to prevent one.



Source: Bill C-36, ss.8, 9, 10(1), 15, 18(5), 62, 70, 121(2)(e), 133. Assessment: Transparency Lab, published by Global Privacy Rights.

Figure 4. The assurance ceiling and the stage profile.

Figure 4. The assurance ceiling and the stage profile. The Act reaches assurance level 3 and cannot reach level 4. Each stage is rated on the ordinal ANCR TPI scale; no composite is given. Source: Bill C-36, ss.8, 9, 10(1), 15, 18(5), 62, 70, 121(2)(e), 133.

Comparative Analysis Framework

This report audits transparency and consent requirements in Bill C-36 against four instruments:

1. **Quebec Law 25**, Canada's most modern provincial privacy law, enforceable since 22 September 2023
2. **EU GDPR**, Regulation 2016/679
3. **Convention 108**, in force with 55 Parties, and **Convention 108+** (CETS 223), which is **not yet in force** at 34 of the 38 ratifications required
4. **PIPEDA**, the statute Bill C-36 replaces in its private sector application

Stage 1: Identity

Which identifiers the Act reaches

Finding. Section 2(1) reaches information about an identifiable individual, including inferred information. This closes the gap that let profile and inference outputs sit outside the definition.

Gap. The threshold remains identifiability. Metadata that does not identify an individual, and that is where surveillance operates, is outside the Act by definition. The Act does not

reach the network and device relationship through which identification occurs before any account exists.

De-identified information is defined as retaining risk. Section 2(1) defines de-identify as modification so that an individual cannot be **directly** identified, expressly stating that a risk of identification remains. Section 63(2) then removes the access right in respect of de-identified information, and sections 20, 21 and 22 permit de-identification, internal research and prospective business transactions without knowledge or consent. The Act therefore creates a category that carries residual re-identification risk and attracts no individual visibility.

Accountability analysis

Finding. Section 8(1) states that an organization must designate one or more individuals responsible for its obligations, and must provide that individual's business contact information **to any person who requests it**.

This is identical to the clause assessed in the 2024 report on Bill C-27. It is a pull obligation. Nothing is published, nothing is resolvable, and nothing is available before a request is made.

Comparison.

GDPR and Convention 108+. Articles 13 and 14 require the identity and contact details of the controller, of any representative, and of the data protection officer, as a condition of lawful processing. The obligation is a push obligation attached to collection.

Quebec Law 25. Section 3.1 requires the title and contact information of the person in charge of the protection of personal information to be **published on the enterprise's website**.

Bill C-36. Section 62(2)(g) requires that the business contact information of the individual to whom complaints may be made be made available. Neither section 8 nor section 62 requires the identity of the controlling organization itself, and neither attaches to the moment of collection.

Adequacy analysis. Because the controller is not identified before processing begins, it is not operationally possible for an individual to know who is asking, under what authority, at the time the question matters. This is not adequate against Quebec Law 25 domestically, and it is not adequate against Articles 13 and 14 internationally.

Stage rating: -1, present but obstructed. Section 12(3) and section 15(3) raise this materially above the 2024 assessment of Bill C-27, so the identity elements are present rather than absent. The contact under section 8(1) is available only on request, and the controlling entity is named at no point, so what is present is obstructed.

Stage 2: Surveillance

What observation the Act permits

Finding. Section 15(1) makes consent the default. Sections 18 to 50 then set out the exceptions, and they are extensive.

- **Section 18(2)**, business activities, permits collection and use without knowledge or consent where a reasonable person would expect it.
- **Section 18(3)**, legitimate interest, permits collection, use **and disclosure** without knowledge or consent where the interest outweighs foreseeable adverse effect. Legitimate interest without required notice is un-governed surveillance. (Like the USA)
- **Section 19** permits transfer to a service provider without knowledge or consent.
 - **Secondary purpose of use without notice is “mass surveillance”**
- **Section 14(2)** lists the circumstances in which information may be used or disclosed for a purpose other than the recorded one, and the list runs to more than thirty sections.

A limit worth naming. Sections 18(1)(b) and 18(3)(b) both exclude collection, use or disclosure **for the purpose of influencing the individual’s behaviour or decisions**. Applied as written, this removes behavioural advertising from both exceptions and is a stronger provision than its GDPR equivalent.

Openness and transparency analysis

Finding. Section 62(1) requires an organization to make readily available, in plain language, information explaining its policies and practices. Section 62(2) adds seven required items: the type of information under control, a general account of use and of reliance on consent exceptions including legitimate interest, a general account of automated decision system use, **whether or not** information is transferred interprovincially or outside Canada, retention periods for sensitive information, how to request disposal or access, and a complaints contact.

Gap. Four defects survive.

1. **No timing.** Readily available is not before collection. Nothing binds the disclosure to the processing event.
2. **General account.** Sections 62(2)(b) and (c) require a general account, not the operative purpose, the legal authority, or the specific processing.
3. **Cross-border disclosure is binary.** Section 62(2)(d) requires whether or not transfers occur. Not to whom, not to which jurisdiction, not under what instrument. An individual cannot determine what legal regime their information has entered.

4. **No version and no evidence.** Nothing requires the disclosure to be versioned, hashed, retained, or recorded as an event. There is no way to establish later what was shown on a given day.

Section 63(3) permits an organization to respond to an access request with the **types** of third parties rather than their names.

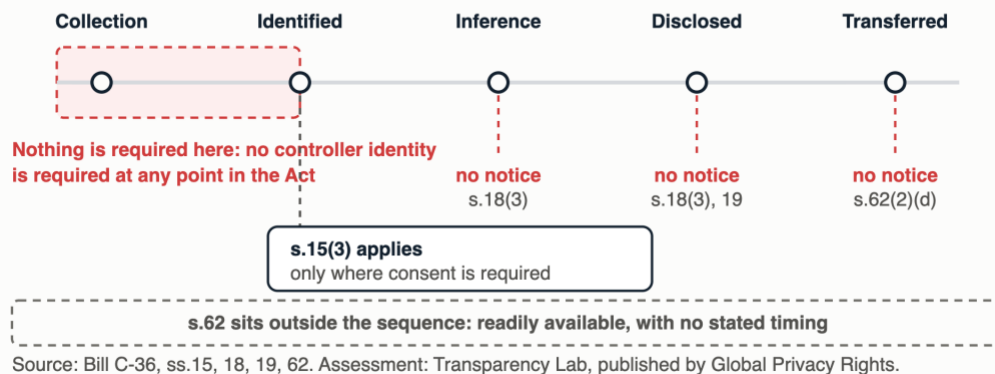


Figure 3. Where the Act places notice in the identification sequence. Nothing is required before identification, and section 62 sits outside the sequence because it carries no timing.

Figure 3. Where the Act places notice in the identification sequence. Nothing is required before identification, and section 62 sits outside the sequence because it carries no timing.

Digital Commons observation. Bill C-36 requires an organization to record its purposes under section 12(3) and its legitimate interest assessment under section 18(5), and to disclose both to the Commission on request under sections 10(1) and 18(5). Every record the Act creates is a controller-held record whose reader is the regulator. The Act creates no record whose reader is the individual.

This is the distinction between a record of processing activities, which is an internal inventory owed to a supervisory authority, and an online notice, which is the disclosure owed to the person. Bill C-36 legislates the first and omits the second, which means indirect data collection is without notice.

Stage rating: 0, present but static or out of context. Section 62(2) is a real advance on Bill C-27 and requires seven disclosures. None is bound to a processing event, versioned, or timed, so the information is present and out of context.

Stage 3: Security of the Surveillance

This stage asks whether the authorised access the Act creates is accountable. It is assessed against four tests: credentialed at the point of request, logged to a party that is not the requester, actively approved rather than standing, and bounded in time and scope.

Bill C-36 materially expands authorised access, which is what makes this stage the decisive one.

Standing access, no threshold

Section 10(1). An organization must, **on request**, provide the Commission with access to its privacy management program. There is no grounds requirement, no notice, and no limit on frequency.

Section 18(5). The same standing access applies to the legitimate interest description and privacy impact assessment.

Neither is credentialed at the point of request, neither is independently logged, and both are standing rather than approved. Against the four tests, both fail three.

Threshold access

Section 118. The Commissioner may audit on reasonable notice, at a reasonable time, and on reasonable grounds to believe a contravention has occurred, is occurring or is likely. There is a threshold, and it is the Commissioner's own satisfaction rather than an external authorisation.

Section 119. The Commissioner may require the organization to commission a report from an approved third party, **at the organization's cost**.

Section 121(2). In proceedings the Commission may compel evidence as a superior court of record, order retention, **enter any premises other than a dwelling house**, converse in private with any person on those premises, and examine or copy records found there. No warrant is required.

Section 121(3) requires records to be returned within a reasonable time and expressly preserves the power to require them again.

Section 120 provides a report to the audited organization, and section 83 requires the Commission to report annually. The audited party learns; there is no per-request log to an independent party, and the individual whose information was examined is never told.

Cross-border access

Section 82 governs disclosure to a foreign authority, and it is the best drafted provision in the Act on this stage.

- Section 82(3) permits disclosure **only** under a written arrangement that limits disclosure to what is necessary, restricts use to the original purpose, and prohibits onward disclosure without the Commission's express consent.
- Section 82(1) expressly **excludes** information received under section 10(1) from foreign disclosure.

Against the four tests, section 82 is credentialed by written arrangement and bounded in purpose and use. It is not logged to a party outside the arrangement, and it is standing rather than approved per request. The individual is not notified at any point.

Determination

The Act reaches assurance level 3 and cannot reach level 4.

Level 3 is met for the foreign disclosure pathway: accountability traces to a named party under a named instrument, and section 82(3) makes the instrument a condition of the disclosure.

Level 4 is a property of the request rather than of the paper, and no access pathway in the Act carries the four properties. Sections 10(1) and 18(5) grant standing access with no threshold. Section 121(2)(e) permits entry without external authorisation. No pathway is logged to a party that is not the requester, and no pathway notifies the individual.

Because a statute sets the ceiling for every contract beneath it, no contract made under the Protecting Privacy and Consumer Data Act can claim dynamic secure level 4, regardless of what the controller implements.

Stage rating: -3, non-operable. Section 82(3) is well drafted and binds the Commission. Measured for rights access, which is where the TPI method tests performance, the stage is non-operable: standing access under sections 10(1) and 18(5), warrantless entry under section 121(2)(e), no notice to the individual at any point, and under section 70(6) an access request that returns nothing while notifying the accessing party that it was made.

Stage 4: Privacy Risk

Recorded, not resolved.

Risk	Basis	Rating
Individual cannot identify the accountable party before identification	ss. 8(1), 15(3), 62(2) contain no controller identity requirement	High
Individual holds no evidence of what was disclosed	No receipt, notice record or notice event log in the Act	High
Cross-border exposure is	s. 62(2)(d) requires a binary	High

Risk	Basis	Rating
unknowable to the individual	answer only	
De-identified information carries residual re-identification risk with no access right	s. 2(1) de-identify, s. 63(2)	Medium to high
Standing regulator access without threshold or independent log	ss. 10(1), 18(5)	Medium to high
Legitimate interest disclosure without knowledge or consent	s. 18(3) permits disclosure, not only collection and use	Medium
Purpose drift through the exception list	s. 14(2) cross-references more than thirty sections	Medium
Automated decision explanation is on request and after the fact	s. 63(4) to (6)	Medium

Consent Validity Analysis

The Kantara Transparency Performance Indicators were applied to the operational viability of consent as drafted.

Section 15(3) is a substantial advance. For the first time in a Canadian federal bill, consent is invalid unless purposes, manner, foreseeable consequences, information type, and third party names or types are provided at or before the moment consent is sought.

Consent remains operationally unprovable. Section 15(3) states what must be provided. Nothing in the Act requires that the provision be recorded, versioned, or evidenced. An organization that complies perfectly, and an organization that does not comply at all, produce identical records: none. This act does not modernize consent, but derogates the highest consent standard and the greatest opportunity for the Canadian privacy and security market.

The consequence is asymmetric in one direction. Under section 114 the Commission may penalise at 3 per cent of gross global revenue. To do so it must establish what an individual was told. The Act gives it the organization's own account and nothing else.

A regulator with order making power needs evidence it can act on. Bill C-36 gives it authority without giving it an evidentiary base that is independent of the party under investigation.

Implementation Capacity

A statute is implemented by people. This section assesses whether Bill C-36 creates the function that would carry it.

The designated individual

Finding. Section 8(1) requires designation of one or more individuals responsible for matters related to the organization's obligations, and provision of that individual's business contact information on request.

What the Act does not require.

Element	Bill C-36	Quebec Law 25	GDPR
Trigger for appointment	Universal, no threshold	Universal	Arts. 37(1)(a) to (c)
Default holder	None specified	Person exercising the highest authority, s. 3.1	Not specified
Seniority floor	None	Highest authority unless delegated in writing	Reports to highest management, Art. 38(3)
Qualification	None	None expressly	Expert knowledge, Art. 37(5)
Independence	None	None expressly	Art. 38(3)
Publication of identity	None	Title and contact published on the website, s. 3.1	Contact details published, Art. 37(7)
Protection from dismissal	None	None expressly	Art. 38(3)

Consequence for the Act's own machinery. Section 9 requires a privacy management program covering protection of information, handling of requests and complaints, staff training, and explanatory materials. Section 10(1) makes that program disclosable to the Commission on request. Section 18(4)(b) requires a privacy impact assessment before any legitimate interest processing. Section 119 permits the Commissioner to require a third party report at the organization's cost.

Each of these presupposes competence inside the organization that the Act does not require it to have. The act deregulates the Canadian professional privacy industry, crippling the governance capacity.

Consequence for the individual. Because the designated individual's contact information is available only on request, and because the organization itself is never required to

identify the controlling entity, there is no published route into an organization for a person who wants to ask who is accountable. Quebec solved this in one sentence by requiring website publication. Bill C-36 does not adopt it.

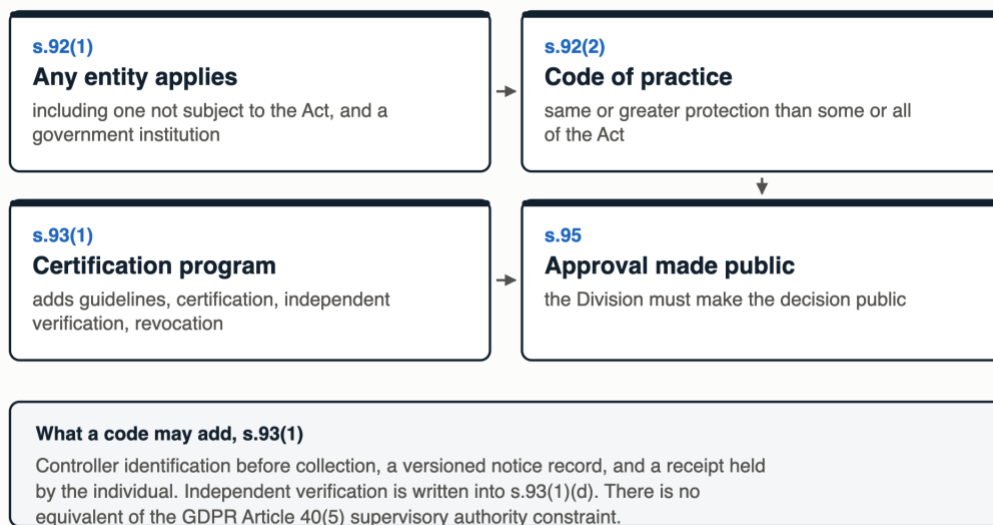
Stage rating: -1, present but obstructed. A designated individual exists and a contact is obtainable, so the function is present rather than absent. It carries no qualification, independence, seniority, publication or dismissal protection, and the contact is available only on request. Section 8 is a contact point obligation carried forward from PIPEDA Schedule 1 that has not developed in twenty five years, while the enforcement attached to it has grown to 3 per cent of gross global revenue.

Codes of Practice and Certification Programs

This is the most significant opportunity in the Bill and it has attracted the least attention.

Sections 92 to 96 create a statutory route for approved codes of practice and certification programs.

- **Section 92(1)** defines entity to include any organization **regardless of whether it is an organization to which this Act applies**, and includes a government institution.
- **Section 92(2)** permits application for approval of a code providing substantially the same or greater protection as some or all of the Act.
- **Section 93(1)** permits approval of a certification program that includes the code, interpretation guidelines, a certification mechanism, **a mechanism for independent verification of compliance**, and disciplinary measures including revocation.
- **Section 95** requires approval decisions to be made public.
- **Section 96** confirms that compliance with a code does not relieve an organization of its statutory obligations.



Source: Bill C-36, ss.92 to 96. Assessment: Transparency Lab, published by Global Privacy Rights.

Figure 5. The route opened by sections 92 to 96. Any entity may apply, including one not subject to the Act, and independent verification is written into section 93(1)(d).

Figure 5. The route opened by sections 92 to 96. Any entity may apply, including one not subject to the Act, and independent verification is written into section 93(1)(d).

Three consequences follow.

1. **Canada acquires a code ownership route that does not depend on the applicant being a regulated organization.** The GDPR Article 40(5) requirement for a competent supervisory authority in the European Economic Area has no equivalent constraint here.
2. **Independent verification is written into the statute**, at section 93(1)(d). A code that specifies inspectable artefacts is directly implementable against that paragraph.
3. **A code may provide greater protection than the Act.** The evidentiary defects identified in this report, controller identification before collection, a versioned notice record, and a receipt held by the individual, are precisely the kind of greater protection section 92(2) contemplates.

The defect this report identifies at the statutory level is remediable at the code level, under the Act as drafted.

Recommendations

To Parliament, at committee:

1. **Add controller identification before collection, to make online notice and consent enforceable.** Amend section 15(3) to require the identity and contact details of the controlling organization, not only its designated individual's business contact information on request.
2. **Require the notice event to be recorded.** Amend section 12(3) so that the recorded purposes are bound to a versioned notice, retrievable at a stated past time.
3. **Give the individual evidence.** A notice receipt, obtainable without an account and without identification, generated at the disclosure event.
4. **Make cross-border disclosure specific.** Amend section 62(2)(d) to require the jurisdiction and the instrument relied upon, not whether or not a transfer occurs.
5. **Close the de-identification gap.** Condition sections 20, 21 and 63(2) on a stated re-identification risk threshold, given that section 2(1) concedes the risk remains.
6. **Log regulator access independently.** Sections 10(1) and 18(5) grant standing access. Require each access to be recorded to a party that is not the requester.
7. **Name third parties.** Remove the types alternative from sections 15(3)(e) and 63(3).
8. **Create the privacy officer function.** Amend section 8 to adopt the Quebec Law 25 model: the person exercising the highest authority is responsible by default, delegation is in writing, and the title and contact information are **published**. Without this, the Act's own privacy management program, privacy impact assessment and audit provisions have no required holder.

To Canada, on adequacy:

9. **Accede to Convention 108+.** Bill C-36 does not close the Articles 13 and 14 gap, and adequacy is assessed against the instrument rather than the penalty.

To implementers, under the Act as drafted:

10. **Use sections 92 to 96.** A code of practice specifying controller identification before collection, a versioned notice record, a notice receipt and a notice event log provides greater protection than the Act, is approvable under section 92(2), is independently verifiable under section 93(1)(d), and is published under section 95.

Methodology

Framework. ANCR Digital Privacy Transparency Compliance and Conformance Assessment Scheme, Kantara Initiative.

Baseline. Convention 108+ adequacy requirements, and ISO/IEC 29100 interoperability with the GDPR and Convention 108.

Source assessed. Bill C-36, 45-1, first reading text as introduced 15 June 2026, retrieved from the Parliament of Canada document viewer. Every clause cited in this report was read

in that text. Bill number, title, sponsor, dates and stage were verified against LEGISinfo. The Bill is at second reading and will be amended; clause numbers are as at first reading.

Standards reference. - Convention 108 (1981) and Convention 108+ (CETS 223, not yet in force) - OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - ISO/IEC 27001:2022 - ISO/IEC 29100, privacy framework - ISO/IEC 29184:2020, online privacy notices and consent - ISO/IEC TS 27560:2023, consent record information structure

Assessment indicators. Kantara Initiative Transparency Performance Indicators applied to controller identification timing and completeness, processing purpose disclosure, legal basis specification, privacy access point availability, and record of processing activity maintenance.

Relationship to the 2024 report. The WHiSSPR Report on Bill C-27 (2024) assessed a bill that is no longer before Parliament. Two of its findings are reproduced here because the clauses they addressed appear in Bill C-36 without amendment. Findings in the 2024 report that do not hold against Bill C-36, including its statement on exemptions, are not carried forward.

Assessment Framework Version: WHiSSPR v2.0 (2026)