

WHiSSPR Comparative: Québec, Canada and China (2026)

Where the individual stands under three transparency instruments

Mark Lizar



Global Privacy Rights

Transparency by Default. Privacy rights that work.

globalprivacyrights.org

SUBMISSION

23 September 2026

WHiSSPR Comparative: Québec, Canada and China (2026)

White Hat Identity, Surveillance, Security, Privacy and Risk (WHiSSPR) Comparative

Full Title: Where the individual stands under three transparency instruments

Author: Mark Lizar

Published by: Global Privacy Rights

Lab: Transparency Lab

Published: 2026

License: Global Privacy Rights, Copyright 2026

Sources compared. Three instruments, each assessed in full on the same method, each with its own published report.

Instrument	Status	Assessment
<i>Act respecting the protection of personal information in the private sector</i> , chapter P-39.1, as amended by Law 25	In force since 2022 to 2024, consolidated text current to 10 June 2026	WHiSSPR Report: Quebec Law 25 Assessment (2026)
Bill C-36, the <i>Protecting Privacy and Consumer Data Act</i> , 45-1	Second reading, House of Commons. Clause numbers as at first reading	WHiSSPR Report: Bill C-36 Assessment (2026)
<i>AI Safety Governance Framework 3.0</i> , TC260, under the guidance of the Cyberspace Administration of China	Guidance, September 2026, revised annually	WHiSSPR Report: AI Safety Governance Framework 3.0 Assessment (2026)

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. - No composite is defined and none should be inferred, within an instrument or across them. Ordinal categories do not support arithmetic, so no instrument is ranked above another by a total. - What is compared is the position the instrument creates for the individual, not the quality of the legal system that produced it.

Scope, and what this report does not assess

This comparative assesses one authority position: the individual's. It asks what a person can inspect, what they are told, when they are told it, and what they hold afterwards.

That is not the only authority position at stake in AI governance. A collective authority position exists alongside it, held by a community over its own data, knowledge, language and territorial information, and it is not reducible to the sum of the individual rights of that community's members. An individual authorisation cannot authorise the use of collective knowledge, and a collective authorisation cannot remove an individual right. Where both apply, both have to be satisfied.

None of the three instruments compared here recognises a collective authority holder at all. That is recorded as a limit of all three, and it is not developed further in this report, because the framework for it has to be defined by the rights holders concerned rather than described on their behalf. Nothing in this report should be read as representing, or as approved by, any community, Nation or people.

Summary

Three instruments, three legal traditions, three stages of legislative maturity. One column is empty in all three.

Québec publishes the name of the accountable person before anyone interacts with the enterprise. Canada records the purposes before collection and brings inference inside the definition of personal information. China builds a tamper-proof, verifiable record of every authorisation, with scoped credentials, mutual recognition between parties, and denial by default.

None of the three gives the individual anything. And none of the three recognises anyone but the individual, so where the interest at stake is collective, there is no authority holder in any of these texts to hold it.

The instruments are not failing at the same task in the same way, which is what makes the comparison worth making. **China built the evidence machinery and pointed it at**

machines. Québec and Canada wrote the rights and built no machinery. One has the mechanism without an addressee. The other two have the addressee without a mechanism.

The comparison in one table

	Québec, Law 25	Canada, Bill C-36	China, Framework 3.0
Accountable party identified to the public before any interaction	Yes. s.3.1 requires the title and contact of the person in charge to be published on the website	No. s.8(1) makes the contact available on request	No. The provider is named, if at all, in the service agreement (5.3.10)
Disclosure bound to the collection event	Yes. s.8, “when the information is collected”	No. s.62(1), readily available, no stated timing	No. Static and contractual
Disclosure before profiling technology is used	Yes. s.8.1, “first inform”	No	No
Purposes recorded before collection	No	Yes. s.12(3)	No
Inference inside the protected category	Partly, through purpose limits	Yes. s.2(1)	Named as a harm at 3.2.4(d), not defined as protected data
A tamper-proof, verifiable record exists	No	No	Yes. Appendix 2, II.3(3), of the operator’s approval of an agent action
A record of the disclosure held by the individual	None	None	None
Superseded versions of the notice retrievable	No	No	No
Log of non-consensual disclosure	Partly. s.18 requires an entry for subparagraphs 6 to 9.1 only	No	Yes, of machine activity. 5.3.6, six months minimum
State access	No. s.18(2), (3), (5)	No. s.70(6) gags the	No reader named for

	Québec, Law 25	Canada, Bill C-36	China, Framework 3.0
recorded and notified	require no entry and no notice	one route back	any record
Individual remedy	Yes. s.93.1, punitive damages of not less than \$1,000	Regulator only	None
Maximum corporate exposure	2% of worldwide turnover (s.90.12); 4% on offence (s.91)	3% of gross global revenue (s.114); 5% on indictment	Not applicable, guidance
A collective or community authority holder recognised	No	No	No
Term “controller”	Zero occurrences	Present as “organization”	Zero occurrences
Term “receipt”	Four occurrences, all procedural	Does not appear	Zero occurrences

1 Identity: who has to say who they are

Québec is alone, and the provision is three sentences long.

Section 3.1 vests the function of person in charge in “the person exercising the highest authority” by default, permits delegation only “in writing”, and then requires that “The title and contact information of the person in charge of the protection of personal information must be published on the enterprise’s website”.

Canada’s equivalent is section 8(1) of Bill C-36, which makes the contact information of the designated individual available on request. The companion assessment records that this clause is carried forward from PIPEDA Schedule 1 and has not developed in twenty five years, while the enforcement attached to it has grown to 3 per cent of gross global revenue.

China’s Framework does not have an equivalent. The words controller, officer and contact appear zero times in TC260’s English text. Responsibility is allocated to roles at 1.3, 5.3.1 and 5.3.12, and the provider is identified to the individual only inside a service agreement, which is presented after identification.

The asymmetry is the finding. China’s Framework requires a tool receiving a request from an agent to verify the agent’s credential and its authorised scope before acting. A person receiving a request for their own data is given no equivalent means of verifying who is asking. Québec closes exactly that gap for humans, and closes it for no machine.

Stage 1 rating Québec **0** Canada **-1** China **-1**

2 The event: when the disclosure is owed

A disclosure that is not bound to an event cannot be checked against one.

Québec binds it twice. Section 8 requires the enterprise to inform “when the information is collected”. Section 8.1 requires an enterprise using technology that can identify, locate or profile to “first inform” the person, and to disclose “the means available to activate the functions”. Profiling is defined in the same section, and the definition reaches work performance, economic situation, health, preferences, interests and behaviour.

Canada does not bind it. Section 62(1) requires information to be made readily available, with no stated timing, and the companion assessment finds that section 62 sits outside the identification sequence entirely for that reason. Section 15(3) sets five items before consent is sought, and applies only where consent is required.

China routes it through the contract. Section 5.3.10 protects “the right to be informed, the right to choose, and the right to supervise” and routes the disclosure through “contracts or service agreements”. A service agreement is presented at sign-up, after identification, and is static.

What Québec proves is that event-bound disclosure is administrable. It has been the law for a private sector of roughly 270,000 enterprises since 2023, and the objection that notice cannot be tied to a processing event is answered by the fact that a jurisdiction did it.

Stage 2 rating Québec 0 Canada 0 China 0

All three sit at 0 for the same reason, and it is the reason this comparative exists: present, and unrecorded.

3 The record: the column that is empty three times

This is the finding.

Québec. The word receipt appears four times in Law 25. Every one concerns the receipt of a request or of a decision. One of them is section 54, which requires the Commission to send its decision to the parties “by any means providing proof of the date of receipt”. So the Act requires proof of receipt when the regulator communicates with a party, and requires none when an enterprise gives notice to an individual. Section 32 runs the thirty day clock from “the receipt of a request” for the same reason. The concept is in the statute. It is reserved for the institutions.

Canada. The word receipt does not appear in Bill C-36 at all. Section 12(3) requires purposes to be determined and recorded at or before collection, and the record is held by

the organization and disclosed to the Commission on request. Section 15(3) requires five items to be provided before consent is sought, and requires no record that they were.

China. The Framework has the most developed record system of the three, and it records the wrong event. Appendix 2, II.3(3) requires human approval records to be preserved “using tamper-proof and verifiable methods”. Section 3.2.1(b) requires “mandatory human approval at critical points and complete records of human approval logs”. Appendix 2, II.2(3) requires “standardized dynamic authorization credentials to enable mutual recognition and interoperability among relevant parties”, verified by the recipient, revoked when the task ends. Appendix 2, II.3(4) denies the operation by default where approval fails.

That is an interoperable, verifiable, scope-bound, default-deny authorisation record system. It records the operator’s approval of a machine’s action. It does not record what the individual was told or what they agreed to.

WHAT EACH INSTRUMENT REQUIRES			
	Québec Law 25, in force	Canada C-36, 2nd reading	China TC260 3.0, guidance
Accountable party named publicly before any interaction	✓ s.3.1	✗ s.8(1), on request	✗ zero occurrences
Disclosure bound to the collection event	✓ ss.8, 8.1	✗ s.62, no timing	✗ service agreement
A tamper-proof, verifiable record exists at all	✗	✗	✓ App.2 II.3(3) of the machine
A record of the disclosure held by the individual	none	none	none
Three traditions, three stages of maturity. The same column is empty in all three.			
Sources: Québec chapter P-39.1 ss.3.1, 8, 8.1; Bill C-36 ss.8(1), 62; TC260 AI Safety Governance Framework 3.0, 5.3.10, Appendix 2 II.3(3). Assessment: Transparency Lab, published by Global Privacy Rights.			

Figure 1. What each instrument requires, and the row that is empty in all three. Québec names the accountable party publicly and binds the disclosure to the collection event. China holds the only tamper-proof verifiable record, and it records a machine’s authorisation. No instrument gives the individual a record of what they were told.

Figure 1. What each instrument requires, and the row that is empty in all three. Québec names the accountable party publicly and binds the disclosure to the collection event. China holds the only tamper-proof verifiable record, and it records a machine’s authorisation. No instrument gives the individual a record of what they were told.

Stated plainly across all three: a service that obtains consent correctly and a service that never obtains it produce the same evidence for the individual, which is none. In China, a service that lets an agent delete a file leaves a tamper-proof trace.

4 Who may read what is recorded

The third WHISSPR stage asks whether authorised access is accountable, not whether unauthorised access occurs.

Québec requires an entry, for the wrong routes. Section 18, second paragraph: “A person carrying on an enterprise must make an entry of every communication made under subparagraphs 6 to 9.1 of the first paragraph.” Those are compulsion, research, debt recovery and recovery of the enterprise’s own claim. The routes that carry personal information to the Director of Criminal and Penal Prosecutions, to police, and to public bodies are subparagraphs 2, 3 and 5, and require no entry. The entry that is required is held by the enterprise making the disclosure, and nothing requires it to be shown to the person concerned.

Section 3.5 is the instructive contrast. Québec will compel an enterprise to tell an individual that their information escaped, and will order the notification where it is not given. It does not require the enterprise to tell them that the information was handed over.

Canada closes the route back. The companion assessment records four routes carrying information to a foreign authority and one route by which an individual might learn of it, blocked by the section 70(6) gag. Section 62(2)(d) reports whether or not a transfer occurred, not to whom, not to which jurisdiction, and not under what instrument.

China names no reader. The Framework requires logs of “system and user activities” retained “for at least six months” at 5.3.6, a floor with no ceiling, and names no reader for most of the records it requires and no condition on access to any of them.

Stage 3 rating Québec **-1** Canada **-3** China **-3**

Québec is above the others here only because an entry requirement exists at all.

5 The remedy, and why it is hard to exercise

Québec gives the individual the strongest position and the least to stand on.

Section 93.1: where an unlawful infringement is intentional or results from gross fault, “the court shall award punitive damages of not less than \$1,000”. A floor, not a discretion. Section 14 closes with “Consent not given in accordance with this Act is without effect”, which voids the consent rather than merely penalising the taker. The Commission may inquire on an anonymous complaint (s.81), may demand documents from any person “whether subject to this Act or not” (s.81.3), and reprisals against complainants are forbidden and presumed from adverse employment measures.

Canada's remedies run to the regulator. China's Framework creates no remedy, being guidance.

So the individual in Québec may sue, and must prove a negative about a disclosure that left no artefact, against a counterparty holding its own policies, its own impact assessments and its own section 18 entries.

Québec gives the individual a cause of action and nothing to bring to it. That sentence is the reason a record matters, and it is more persuasive in the jurisdiction with the strongest rights than in the jurisdictions with the weakest.

Stage 4 rating	Québec -1	Canada -1	China, not rated, guidance
----------------	-----------	-----------	----------------------------

6 What each has that the others lack

Instrument	The thing it has	The thing it is missing
Québec	A published accountable identity, before identification, and a disclosure bound to the collection event	Any artefact proving either happened
Canada	Purposes recorded before collection, inference inside the protected category, and a statutory route to approved codes of practice with independent verification	Timing, identity, and any record for the individual
China	An interoperable, tamper-proof, scope-bound, default-deny authorisation record system	An addressee. Every record it builds is read by the operator, the auditor or the state

Read down the middle column and the pieces of a working system are all present, distributed across three jurisdictions that are not going to converge by agreement. Read down the right column and the same element is missing three times.

7 What would close it, and it is small

Each instrument is one change away, and none of the three requires a new principle.

Québec. Require the section 8 disclosure to reference the version of the section 8.2 confidentiality policy in force at that moment, and to be issued to the person as a record they keep. Section 3.3 already requires projects to allow personal information to be communicated “in a structured, commonly used technological format”, so machine-readable output is already contemplated. Section 3.5 already shows that notice content can be prescribed by government regulation.

Canada. Bill C-36, sections 92 to 96, opens a route that requires no amendment at all. Any entity may apply, including one not subject to the Act. A code may offer the same or greater protection than some or all of the Act. Independent verification is written into section 93(1)(d) and the approval decision is made public under section 95. There is no equivalent of the GDPR Article 40(5) constraint requiring a supervisory authority. A code of practice specifying controller identification before collection, a versioned notice record and a receipt held by the individual can be approved through that route while the Bill is still in committee.

China. The Framework revises annually and says so. Appendix 2 already specifies the record, the credential and the default-deny rule. Applying them to the individual’s consent rather than only to the operator’s approval produces a record the individual can hold and a recipient can verify. Four clauses invite it: 4.1.2 supports participation in international standard setting, Appendix 2 II.2(3) asks for mutual recognition and interoperability, Appendix 3 principle 7 calls for international mutual recognition of assessment methods, and Appendix 2 commits to continuous updates.

The common structure already exists. ISO/IEC TS 27560:2023 specifies an information structure for a record of a notice and consent event, and ISO/IEC 29184:2020 specifies what a notice must contain. Neither instrument of the three references any ISO/IEC document.

One design consequence follows from the scope note above. A record built only to carry an individual’s disclosure will not carry a collective authorisation, because the two answer different questions: who was told, and who had the standing to permit it. A record structure that is specified once and expected to serve both has to carry the accountable operator, the purpose and the authority relied on as separate fields, so that an authority which is not the individual can be named in the same structure rather than requiring a second one. That is a requirement on the structure. What it should say, and who defines it, is not a question this report answers.

8 Why this is a Canadian argument, and why it starts in Montréal

Canada is in the unusual position of holding both ends of the problem inside its own federation.

The strongest transparency requirement in North America is provincial, in force, and roughly three sentences long. The federal reform bill on the order paper does not contain it. A federal measure that falls below section 3.1 would leave Canadian individuals better protected in one province than in the country, and would leave enterprises operating to two standards.

That is a domestic argument before it is an international one, and it does not require agreement with, or criticism of, any other jurisdiction to make. It requires only the observation that Québec already does the thing, and that the record which would make it provable does not exist anywhere.

The international position follows from it rather than leading it. Convention 108 is in force with 55 Parties, and Convention 108+ stands at 34 of the 38 ratifications required. An instrument that produces a portable, verifiable record of a disclosure is the kind of thing that can be recognised across those Parties, because what travels is the record structure rather than the statute. The comparison in this report shows that the three instruments cannot be harmonised as texts and can interoperate as evidence.

Impact

For individuals. In all three jurisdictions the individual is asked to do the checking and is given nothing that can be checked. Québec asks the least of the individual and still places the entire evidential burden on them.

For enterprises. The marginal cost of issuing a record alongside a notice already required is small against obligations already carried: Québec's impact assessments under sections 3.3 and 17, Canada's recorded purposes under section 12(3), China's approval logs under Appendix 2. In each case the hard part is built and the record is the cheap part.

For regulators. A supervisory authority currently learns what an organisation disclosed by asking the organisation. A record referencing a published version, timestamped at the event, changes supervision from correspondence into inspection, and it does so without requiring the authority to hold more personal data.

For cross-border cooperation. Québec's section 17 already assesses the legal framework of the receiving State before a transfer, which is the analysis transborder cooperation needs, and keeps the result private. Canada reports only whether a transfer occurred. China offers a counterparty outside its jurisdiction no controller identity and no disclosure of location. A record that names the accountable party, the version disclosed and the jurisdiction is the smallest artefact that makes any of these three legible to the others.

Recommendations

To the Government of Québec. Require the section 8 disclosure to carry a version reference and to be issued to the person concerned as a record. Extend the section 18 entry requirement to the state routes at subparagraphs 2, 3 and 5. Remove the browser cookie exemption at section 9.1 or bound it.

To the Government of Canada. Do not legislate below section 3.1 of the Québec Act. Require the accountable organisation to be identified in a published and retrievable record before an interaction begins, require disclosures to be versioned and superseded versions retained, and give the individual a receipt of the disclosure obtainable without an account or identification. Use the route at sections 92 to 96 to approve a code of practice carrying these measures without waiting for the Bill.

To TC260. Extend the tamper-proof, verifiable record at Appendix 2, II.3(3) to notice and consent events and give the individual a copy. Specify the standardised dynamic authorisation credential against ISO/IEC TS 27560:2023, so that agent authorisations and individual consents share one recognisable structure across borders.

To standards bodies. The three instruments differ in tradition, in enforceability and in what they protect. They do not differ in what they omit. A record structure specified once and referenced by each is the only element that could be adopted by all three without any of them adopting the others' law.

Methodology

Each instrument was read in full in its official text and assessed on the WHiSSPR stages in order, with the stage rating fixed before the next stage was asked. Term counts were taken across each whole text. The three assessments were produced separately and are published in full; this comparative draws only on findings recorded in them, and adds no finding that is not traceable to one of the three.

Ordinal ratings are compared as categories. No composite is given for any instrument and none is given across them.

Unresolved

Item	Status
Whether the Chinese text of Framework 3.0 differs in substance from TC260's English text at the clauses cited	Not checked. Where they could differ, the Chinese text governs. This limit applies to every statement about the Framework in this report

Item	Status
Whether the French text of chapter P-39.1 differs in legal effect at the clauses cited	Not checked. Both versions are official
Bill C-36 clause numbers	As at first reading. They will move in committee
Whether the Québec section 27 access right reaches the section 18 entries	Not stated in the Act, and no decision of the Commission on the point was sought
Decisions applying any of the three instruments	Not surveyed. This comparative assesses the instruments, not their application
Convention 108 Parties and Convention 108+ ratifications	Checked. Council of Europe Treaty Office, 23 September 2026: ETS 108 shows 55 ratifications or accessions and no signature outstanding; CETS 223 shows 34 ratifications and 12 signatures not followed by ratification, against the 38 required

Companion reports

All three assessments are published in full by Global Privacy Rights and are available at <https://globalprivacyrights.org/research>.

- WHiSSPR Report: Quebec Law 25 Assessment (2026)
- WHiSSPR Report: Bill C-36 Assessment (2026)
- WHiSSPR Report: AI Safety Governance Framework 3.0 Assessment (2026)

Assessments conducted by Transparency Lab, the Global Privacy Rights lab, and published by Global Privacy Rights as publisher of record.

© 2026 Global Privacy Rights.

Assessment Framework Version: WHiSSPR v2.0 (2026)