0PN-DTL WHiSSPR Report: Assessing Governance Capacities of Bill C27

Mark Lizar & Gigi Agassini

Licence: 0PN-Digital Transparency Labs Copyright 2024

0PN-WHiSSPR: Bill C27 Report

Assessment Summary

Upon assessing Bill C-27 the act to enact the Consumer Privacy Protection Act.

The report assesses the operational usability of Bill C-27 to control personal data, evaluating whether the transparency required in the legislation is valid or adequate with GDPR, Quebec Law 25, and Council of Europe Convention 108+,[1] to report on the international adequacy with the Commonwealth.

Reporting

The transparency requirements found in Bill C-27 are lacking operational accountability, meaning this legislation is unsuitable for individuals to operationally control their own data. The Bill does not indicate that the Controller's identity is required to be '*provided*' nor is notice required when individuals are being surveilled.

In addition, there is insufficient required openness to provide a notice or sign, notification or disclosure when using surveillance technologies. or to implement or maintain a state of notice for meaningful consent,[2] nor is there a requirement to make a record of notice or consent. Also lacking is the requirement for a data privacy officer in accordance, or accountable service representative, to address privacy and security risks.

Instead, BillC27 stipulates analogue privacy administration, entrenching 1998 PIPEDA transparency requirements for analogue privacy governance measures, including a Tribunal to adjudicate matters of privacy governance, which would be the first of its kind.

This short report utilises the Kantara ANCR WG, Digital Privacy Transparency Assessment Scheme[3To] assess the operational viability of consent as presented in Bill C-27. This has revealed in short order that while consent is presented in the legislation, it is not presented in a manner which is legally valid, in that it doesn't require a minimum operational level of accountability and transparency for consent to be legal or valid under Bill C-27.

A high-level analysis of Bill C-27 indicates a US style Consumer Protection Regulation, not privacy legislation in which consent is the default, not reflecting privacy as a fundamental right, which Canada has long championed in the Commonwealth.

> Recognition of the importance of the accountability principle has increased over time. Domestic privacy laws have come to introduce a variety of mechanisms designed to promote the accountability of both

[1] Council of Europe (2018), "Convention 108 + Convention for the protection of individuals with regard to the processing of personal data",[Internet]https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (accessed

[2] Meaningful Consent, Office of Privacy Commissioner of Canada, https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/info_mc/

[3] ANCR WG, 2023 Kantara Initiative "ANCR Digital Privacy Transparency Compliance and Conformity Assessment Scheme" [Internet]https://kantara.atlassian.net/wiki/spaces/WA/pages/301564731/ANCR+Digital+Privacy+Transparency+Compliance+and+Conformity+Assessment+Scheme

public and private data controllers. Obligations of transparency towards individuals and privacy enforcement authorities are clear examples of such mechanisms. [4]

Resulting Analysis

Bill C-27 does not represent what Canadians expect The lack of digital security and privacy afforded is not consistent with the Charter of Rights and Freedoms, Section 7,[5] which guarantees everyone the right to life, liberty and security of the person. (Including security from surveillance)

While consent features prominently in the legislation, the transparency and accountability clauses, when reviewed using the Kantara ANCR Transparency Performance Scheme, indicate that the consent would not be adequate or valid in use. This reveals a consumer protection legal framework that is inadequate as privacy legislation and not adequacy with transborder digital consent requirements.

If you have any further questions or need additional assistance, in adequate with;

- Quebec Law 25 (formerly Bill 64)[6]
- R v Jarvis, [2019][7The] 2 SCR 406 Supreme Court decision on the expectation of privacy in public
- Bill C27 is not adequate for data- transfers and transborder governance.

Furthermore, there is credible concern of the impact this legislation will have on the future of Canadian data sovereignty, security, and digital privacy infrastructure.

Impact on Canadian Industry

Bill C-27' security clauses, the authentication clauses further de-regulates the use of digital identity for surveillance based profiling. This threatens existing Canadian public private partnerships evolving to govern in this space. In particular the Pan-Canadian Trust Framework,[8] in effect de-regulating authentication undermining governance of digital by lowering the governance bar dramatically,[9] how we are authenticated, this undermines our digital security and national sovereignty.

---

[4] Robinson, L., K. Kizawa and E. Ronchi (2021), "Interoperability of privacy and data protection frameworks", OECD Going Digital Toolkit Notes, No. 21,

[5] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11. [Internet] https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/pdf/charter-poster.pdf

[6] Bill 64 (2021, chapter 25), An Act to modernise legislative provisions as regards the protection of personal information, September 23, 2021. Now referred to as Law 25, An Act to modernise legislative provisions as regards the protection of personal information, SQ 2021, c 25.

[7] R v Jarvis, [2019] 2 SCR 406 [Internet] https://www.scc-csc.ca/case-dossier/cb/2019/37833-eng.pdf

[8] Digital ID & Authentication Council of Canada (DIACC), "The Pan-Canadian Trust Framework," August 11, 2016, https://diacc.ca/2016/08/11/pctf-overview/.

[9] Bill C-27, Clause 57(3)

To address the issue and to support Canada's position in the Commonwealth as a leader in democratic values, ethics, and the separation of powers.[10] We append to this short report a Digital Privacy & Trust Capacity Assessment for legislation and regulation comparison in the Commonwealth.

WHiSSPR Report

In 0PN-DTL digital privacy transparency research, requirements for notice, notification and disclosures are assessed and recorded, using standard consent record information structure..

This is significant for understanding the validity, technical operability, and integrity of consent as a mechanism for data control.

This report is based on an analysis of adequacy against, 23 transparency, notice, notification, and disclosure requirements identified in the GDPR and Conv 108+. reflected in Chapter 1 transparency modalities for consent to be used for legal data control adequacy.

For consent to be legally compliant, notice of who you are consenting too is an operational requirement and a sovereign data governance requirement to assert for *any* legal justification to use surveillance technology, in the Commonwealth in reference to GDPR and Conv.108+. As assessed here.

Table 1 Accountability

Bill C27	**8 (1)** An organisation 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.	**Not Adequate**
GDPR/108+	The identity of the data controller must be provided [Articles 13, 14] (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable.	The organisation owner is the accountable person, unless there are high risks as defined in regulation, at which point a Data Privacy Officer must be appointed.
Quebec L25	3.1. Any person carrying on an enterprise is responsible for protecting the personal information held by the person. Within the enterprise, the person exercising the highest authority shall ensure that this Act is implemented and complied with. That person shall exercise the function of the person in charge of the protection of personal information; he may delegate all or part of that function in writing to any person.	The owner(s) or senior individuals in any organisation or institution, is accountable, mitigated by delegating this accountability to a data privacy officer (equivalent).

[10] Commonwealth Ministerial Action Group (CMAG) https://thecommonwealth.org/commonwealth-ministerial-action-group

	The title and contact information of the person in charge of the protection of personal information must be published on the enterprise's website or, if the enterprise does not have a website, be made available by any other appropriate means.	
Adequacy Analysis	Canadian privacy law undermines and is not compliant with Quebec Privacy Regulation or Adequate for governing Transborder flows of personal information and the OECD[11]. The identity of the controller, the beneficial owners of the processing personal data are not communicated prior to processing, as a result it is not operationally possible for individuals to consent to data processing, this is not valid legally, adequate with Quebec domestically or internationally in the commonwealth.	

Insufficient transparency in Bill C27 no requirement to *provide* identity of Controller in Notice, notifications or disclosures for privacy, consent and surveillance.

A requirement to identify the controlling organisation and accountable individual is a minimum for accountable data processing.

Non-conformant to standards or compliant to existing regulation, expectations or requirements for consent by default, limiting the validity of all consent clauses and provisions in this bill.

Openness & Transparency

Bill C27 'Openness and Transparency' Section 62 has only 9 clauses, the most significant for being open and transparent is informed by clause 62(1) is extremely vague.

Only plain language that is readily available to explain its practices to each and every explaining policies is required in this privacy law without the identity of the controller, or specific notice over confidentiality of processing. (as required in Quebec)

Notice

Bill C27 -62(1)	**62 (1)** An organisation must make readily available, in plain language, information that explains the organisation's policies and practices put in place to fulfil its obligations under this Act.	**Not Adequate**

[11] OECD. (2021). Recommendation of the Council on Enhancing Access to and Sharing of Data. OECD.org.

GDPR/108+	The identity of the data controller must be provided [articles 13, 14].	Making readily available in plain language, is the same a means that no proof of notice or knowledge is required, which is not sufficient for consent as evidence by decision and May 23rd, fine of Meta[12] in the EU.
Quebec L25	3.1 The title and contact information of the person in charge of the protection of personal information must be published on the enterprise's website or, if the enterprise does not have a website, be made available by any other appropriate means.	3.1. Any person carrying on an enterprise is responsible for protecting the personal information held by the person. Within the enterprise, the person exercising the highest authority shall see to ensure that this Act is implemented and complied with. That person shall exercise the function of person in charge of the protection of personal information; he may delegate all or part of that function in writing to a personnel member.
Adequacy Analysis	Digital Commons Bill C27 - places no obligation on the service to provide any transparency, only requires that the information listed in 62(1) be made available, without a record of notice or processing activities for services online, - for any stakeholder.	

[12] 1.2. Billion Euro Fine - May 22, 2023
https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en
Ruling: I agree to terms, does not constitute legal consent for behaviour advertising, or provide Meta with rights over micro-data aggregations and commercialization.

Digital Privacy Governance Capacity Assessment

In Canada at the moment, a very deceptive privacy legislation has been put forward, which on the surface looks like it is consent by default, but in fact, is not operational or adequate with Convertion108+.

To address misaligned consumer protection and privacy legislation, the rating produced by this assessment is used to educate stakeholders on expected strength, adequacy, integrity and capacity for digital governance in the Commonwealth.

The Governance Capacity Assessment is to rate the extent to which legislation can be assured with a Digital Privacy Credit Rating.

The assessment reviews the sovereign authority and its use in the governance of data, the independence of the National Data Protection Authority, the delegation of this data governance authority to Data Privacy and Surveillance Officers, and the subsequent authority to process this data by 3rd party data processors and sub-processors.

Likewise, data sovereignty in free and democratic societies is delegated to the individual, and their capacity to meaningfully consent to services to use personal data only for the purpose as expected. Delegation of authority in this context comes by citizenship, validated physical locations governed by co-regulation. Assessing international adequacy with Convention 108+ using ANCR mirrored record and receipt standards to scale digital privacy transparency reporting consistently. In this way digital privacy expectations can be measured, even assured between parties.

Assessment Role Acronyms

These roles are mapped to the stakeholders involved, the roles may not be called the same name in various jurisdictions and languages, but are equivalent to roles that require accountability mapped here for clarity.

- DPA - Data Privacy Authority (DPA), refers to privacy regulating authority.
    - Data Privacy Authority, e.g.
- PII Controller – Legal Entity and Owner.
- DPO – Data Privacy (and Surveillance) Officer.

	Bill C27	Adequacy	Reference	Analysis
Is security and privacy a fundamental right?	No	Not Adequate	Part 1, Section 2. "An Act to support and promote electronic commerce by protecting personal information that is collected".	Consent in Bill C27 is not compliant and derogated to business interests and as a result does not secure Canadians against foreign surveillance or protect data sovereignty
Does the legislation apply to all stakeholders and is this equally balanced?	No	Not Adequate	Political parties are not governed or referred to in any section in Bill C27.	Refer to Appendix A, to see assessment analysis.
Is there an equivalent to a presidential secret surveillance backdoor to the regulation?	No	Partially adequate	Part 2, Section 2, refers to " In this Act, Minister means the member of the Queen's Privy Council for Canada designated under section 3 or, if no member is designated, the Minister of Industry."	There is no restriction or explicit restriction on secret government or commercial surveillance. This also puts a tribunal in place which can make regulation, and allow for business to surveil by default, "legitimate interests" to further embed secret mass surveillance.
Is the political class exempt from privacy regulations?	Yes	Not adequate	Yes, there are currently no regulations that govern the use of personal data by politicians	Bill C27 only covers the private sector.
Is the political class subject to, or using tools mass and secret surveillance?	Yes	Not adequate	Political class is subject to, ad participating with multiple tools used to influence Canadians with foreign interference	The use of social media applications on gov phones. Government use of funds to pay for advertising on foreign social media platforms.(ref)(ref SouthPark) Government departments using spyware on employee devices (ref)
Does the political class dictate privacy standard?	Yes	Not adequate	Bill C27 is written and directed by Government Ministers, and their advisors.	The recommendations and
Is digital privacy governance capable?	No	Not Adequate	The addition of a tribunal, rather than requiring records of processing activities makes Bill C27 non-digital capable	The opposite, it adds a layer of analogue governance.

Does a foreign data intermediary service, or a gateway platform service provider, require a DPO representative in the local Jurisdiction?	No	Not Adequate	Services like Google, using IAB, make 14.7 Billion a year off of Canadian personal data.	There are no requirements for foreign services to provide privacy rights services or support local to Canada.
Is there a requirement for DPO's to report privacy violations to DPA?	Private Sector -No Public Sector-Yes	Partially Adequate	Public Servants Disclosure Protection Act, And Conflict of Interest Act, in part do provide reporting requirements, but these are not specified in B ill C27. [13]	There is no requirement for a data privacy officer in Bill C27.
Do DPO/DPA's have or provide any whistleblowing style protections or incentives for reporting to Authority? E.g. 25% of the fine, Are DPA, DPO, Independent from a) the political class?	Private Sector -No Public Sector-Yes	Partially Adequate	Public Sector employees do have whistleblower protections, not specific to data privacy officers.	There is no data-trust safeguards for conformance and compliance in Bill C27.

There are 10 Questions to Assess BillC-27, in order to provide it with a rating for Digital Privacy Trust in Canada.

This assessment reveals that Bill C 27, would achieve a generous, 1.5 out of possible 10, indicating it a score of **15%** well below the 100% required for competitive digital governance capacities. . Bill C27 non-conformance or compliance to security and privacy expectations - Not-Adequate for the digital commons.

In the Commonwealth, regulation must be nationally implemented to ratify adequacy, or the equivalent, and the rights to privacy and security, must be a fundamental right.

Terminology and Acronyms

The digital governance semantics specified here simplify analysis of the adequacy of Bill C27 as regulatory instrument in the Digital Commons, in which privacy as opposed to consumer protection, is a fundamental right in Canada and the Commonwealth.

Quebec Law 25

- ACT RESPECTING THE PROTECTION OF PERSONAL INFORMATION IN THE PRIVATE SECTOR

[13] Bill

- Came into force on Sept 22, 2023.
- Innovates consent regulation to address critical consent usability, implementing consent for primary and secondary purposes, regardless of the legal justification.

Bill C27

- Titled: Digital Charter Implementation Act.
    - Subtitle: **Canadian Consumer Privacy Protection Act.**

ANCR WG

- Kantara Initiative: Anchored Notice and Consent Receipt Work Group at the -

0PN: Digital Privacy Transparency Semantics

- **0PN**: This refers to being open about both a) the legal compliance, b) and conformance of a record to determine the performance in standard way. 0PN = 0pen^2 .
- **Digital**: references specifically cyber security, its data control and protection design gov architecture.
- **Digital Privacy** – Consent by Default, surveillance online.
- **Digital Transparency** - transparency over the security design and data control defaults, context settings relative to consent.
- **Digital Privacy Transparency** – Privacy by design that enables consent by default embeds personal security by design.

Digital Commonwealth + Governance in Canada

- 1931 Statute of Westminster – Canada became a Sovereign nation joined the Commonwealth with Australia, New Zealand, South Africa and free Irish State.
- Charter of Rights & Freedoms.
- 2018 meaningful consent law in Canadian the highest global standard for legal consent was passed, setting consent legal standard in Commonwealth, why Canada might still have Adequacy status with the EU.[14]
- 2019 Jarvis vs Supreme Court- Right to privacy in public.
- In 2020 ISO/IEC 29184 Online Privacy Notice and Consent was published in 2020 and has itself become the basis for a standard.
- 2023, Sept 22nd, Quebec Law 25, consent law became enforceable.
- 2023 ISO/IEC 27560 Consent record information structure, published in August 2023.
- 2024, March 16 – The Digital Services Act Comes into force, the DSA when drafted included the consent receipt.
- 2024 – expected that Council of Europe 108+ will be ratified.

[14] Digital Services Act comes fully into force February 2024,

ANCR Digital Privacy Transparency Compliance and Conformance Scheme

The ANCR WG Compliance and Conformity Assessment Scheme.[15]

Implemented in the 0PN-Digital Transparency Lab, under 0PN-License;

- Compliance refers to the technical Adequacy with Convention 108+ (mirrors the GDPR) international privacy legal framework, which ISO/IEC 29100 is interoperable with. All of the above is driven by the OECD 1980, Guidance for the Protection of in the Transborder Flows of Personal Information,[16] and subsequent OECD Privacy Framework Guidance.
    - This open to access international standard has been developing for 43 years and has been responsible for driving regulatory policy in the Commonwealth.
    - Conformance refers to conformance with ISO/IEC 29100 Security and privacy framework which extends the ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection standard and 29100 is implemented in 74 countries, the most interoperable, and widely used international framework standard. Which makes the ANCR Framework, the only international assessment scheme for digital privacy.

[15] ANCR WG, Kantara Initiative, 2023, Digital Privacy Transparency Compliance and Conformity Assessment Scheme v0.9.1.1, [Internet Dec 2023]https://kantara.atlassian.net/wiki/spaces/WA/pages/301564731/ANCR+Digital+Privacy+Transparency+Conformity+and+Compliance+Assessment+Scheme

[16] 0ECD, 1980:2002. Guidelines for the Protection of in the Transborder Flows of Personal Information, OECD Publishing, Paris, [Internet], https://doi.org/10.1787/9789264196391-en.