0PN: Digital Transparency Lab
Bill C27 Report & Rating

Mark Lizar & Gigi Agassini

0PN - BILL C27: REPORT OVERVIEW 3

INTRODUCTION 5

Bill C27: Accountability for Consent 5
Table 1 Accountability 5

OPENNESS & TRANSPARENCY 6

Notice 6

DIGITAL PRIVACY TRUST ASSESSMENT FOR COMMONWEALTH LEGISLATION 8

Terminology and Acronyms 11

0PN - Bill C27: Report Overview

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

This report assesses the compliance and conformance of Bill C-27, to transparency and consent adequacy requirements, with GDPR, Quebec Law 25, and Council of Europe Convention 108+,[1] for international adequacy with the Commonwealth.

There were no requirements found in Bill C-27 to '*provide*' notice when being surveilled and no requirement to provide a digital notice or identity credential of the PII Controller. Nor are there any requirements for a data privacy officer in accordance with the scale of privacy and security risks. Instead, Bill C-27 entrenches static, 1998 PIPEDA transparency requirements for analogue privacy governance measures, including a Tribunal to adjudicate matters of privacy governance, which would be the first of a kind.

This short report utilizes the Kantara ANCR WG, Digital Privacy Transparency Assessment Scheme[2] to 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.

Our 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 public and private data controllers. Obligations of transparency towards individuals and privacy enforcement authorities are clear examples of such mechanisms. [3]

As a result, not only does Bill C-27 not represent what Canadians expect it is not consent by default, in accordance with; the Charter of Rights and Freedoms, section 7,[4] which guarantees everyone the right to life, liberty and security of the person. (Including security from surveillance).

---

[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] 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.

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

[4] 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

What is referred to as consent in Bill C-27 is easily revealed as in-valid using the ACR Scheme, as there is technically insufficient transparency required for consent, and its accountability. As such, it is categorized as consumer protection legislation that is inadequate with;

- Quebec Law 25 (formerly Bill 64)[5]
- R v Jarvis, [2019][6] 2 SCR 406 Supreme court decision on the expectation of privacy in public
- Bill C-27 is not adequate for data- transfers and governance transborder.

Furthermore, hitting much closer to home, is the impact this legislation would have on Canadian data sovereignty, security, and privacy infrastructure. Bills C-27's authentication clause, de-regulates digital identity surveillance and threatens Canadian public private partnerships evolving to govern in this space. In particular the Pan-Canadian Trust Framework,[7] in effect de-regulating authentication undermining governance of digital by lowering the governance bar dramatically,[8] how we are authenticated, this undermines our digital security and national sovereignty.

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.[9] We append to this short report a Digital Privacy & Trust Capacity Assessment for legislation and regulation comparison in the Commonwealth.

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

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

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

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

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

Introduction

This report utilizes the methodology for evaluating digital identity governance interoperability requirements between Canada and the EU, In the Report on Adequacy of Digital Governance published by DIACC.

In this report 23 transparency, notice, notification, and disclosure requirements are identified for transparency modalities to indicate adequacy. Of these, the requirement to *Provide*, notice of the identity of the controller, including both the legal entity and that of the Data Privacy Officer, as well as digital privacy contact point.

Bill C27: Accountability for Consent

In this 0PN digital privacy transparency research, requirements for notice, notification and disclosures are assessed. This is significant for understanding the validity, technical operability, and integrity of consent mechanism.

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 C-27	**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.	**Not Adequate**
GDPR/108+	The identity of 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 organization 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. With in the enterprise, the person exercising the highest authority shall see to ensuring that this Ac tis 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 any person.	The owner(s) or senior individuals in any organization or institution, is accountable, mitigated by delegating this accountability to a data privacy officer (equivalent).

	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[10]. 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 C-27 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.

This assessment finds that Bill C-27 use of consent is not 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 C-27 '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 controller, or specific notice over confidentiality of processing. (as required in Quebec)

Notice

Bill C27 -62(1)	**62 (1)** An organization 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**

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

GDPR/108+	The identity of 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[11] 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 ensuring 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 C-27 - 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.	

[11] 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 Trust Assessment for Commonwealth legislation

To address misaligned consumer protection and privacy legislation, this rating is used to quickly assess the strength of adequacy, integrity and digital governance capability of any data law or legislation in the Commonwealth.

The Integrity Assessment as 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, and location, and by co-regulation, through international adequacy with Convention 108+ and using international record and receipt standards for digital privacy transparency. In this way digital privacy expectations can be assured between parties (peer to peer) without data intermediaries.

Assessment Role Acronyms

These are generic role types, which may not be called the same name in various jurisdictions and languages, but the local name for accountable person for privacy for a legal entity can be mapped to these terms

- 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 C-27 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 C-27.	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, surveillance 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 C-27 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 intell.	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, using Bill C-27 rather than requiring records of processing activities makes Bill C-27 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 supports 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 Bill C-27. [12]	There is no requirement for a data privacy officer in Bill C-27.
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 are no data-trust safeguards for conformance and compliance in Bill C-27.

There are 10 Questions to Assess Bill C-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% expected for modern national privacy legislation. For International market entry Bill C-27 is non-conformant and non-compliant for security and privacy in 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
    - 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.
        - Sub-Tittle: **Canadian Consumer Privacy Protection Act.**

ANCR WG

- Kantara Initiative: Anchored Notice and Consent Receipt Work Group

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.[13]
- 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.

ANCR Digital Privacy Transparency Compliance and Conformance Scheme

The ANCR WG Compliance and Conformity Assessment Scheme.[14]

0PN-Digital Transparency Conformance and Compliance

- 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,[15] 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.

About 0PN Digital Transparency Lab

Surveillance transparency, Privacy & Consent Standard have been the focus of the research and development for almost 20 years, 0PN has been an evolution of efforts in commons orientated communities, since 2006 when the Identity & Trust WG was first started at Identity Commons,[16] The anthropology of digital Identity ad Trust evolved from the Work Group, into the first ever Community Interest Company called Identity Trust C.I.C. Developing both digital identity and Video Surveillance Registries, before working on a effort standardize digital privacy notice, replace agreements with consent. The Open Notice Initiative launched with a Jan 28 Data Privacy Hackathon in 2012, the work was

[13] The he DSA rules will apply to all platforms from 17 February 2024 [Internet] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

[14] 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

[15] 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.

[16] Lizar, M, Givotosky, Identity Trust WG, 2006 [internet] http://wiki.idcommons.org/Identity_Trust_Charter

thehttps://opennotice.smartspecies.com/w3c-do-not-track-beyond-paper-and-presentation consolidated into working on specifications for ISO/IEC standards first in the Kantara Initiative Consent & information Sharing WG, in 2013.

Where the Consent Receipt v1 was championed, written in conjunctions with ISO 29100 and 29184, to provide an international standard consent record information structure. The Open Consent Group UK, in 2015, then in Notice The Anchored Notice and Consent WG ANCR WG In 2018.

I now published becoming ISO/IEC 27560 Consent record information structure in Aug, 2023. Marking 17 years working on Identity Trust and Consent.

For the latest specifications the Kantara Initiative ANCR WG roadmap provides what is next. Driven by R&D now in the 0PN Transparency Lab Canada.

About ANCR @ the Kantara Initiative

All the invested time and effort from many people, work groups and communities have now evolved into the current Kantara Initiative ANCR WG.

ANCR Roadmap for 2024

- Consensus Collaboration Protocol
- Digital Privacy Transparency Compliance and Conformance Scheme[17]
- PII Controller Notice Credential
- ANCR Record information structure[18]
- AuthC: Digital Identifier Exchange and Interoperability Protocol for Authorization from Consent
    - Consent Receipt v2, Consent Tokens

[17] ANCR Compliance and Conformance Scheme
https://kantara.atlassian.net/wiki/spaces/WA/pages/301564731/ANCR+Digital+Privacy+Transparency+Compliance+and+Conformity+Assessment+Scheme

[18] https://kantara.atlassian.net/wiki/spaces/WA/pages/304480257/ANCR+Record+Information+Structure+v0.7#[inlineExtension][inlineExtension][inlineExtension]Notice-Record-Security