0PN
Digital Transparency Lab

Global Privacy Rights
https://globalprivacyrights.org/

0PN-DTL WHISSPR REPORT

Assessing Governance Capacities of Bill C27

AUTHOR
Mark Lizar

EDITED BY
Gigi Agassini

Bill C-27, A critical threat to privacy, security and data sovereignty

Contents

About WHiSSPR

A WHiSSPR Report is an audit of the privacy and security of identity surveillance. It is an assessment that is used to assess the security of surveillance, who the risk owners are and the overall risk surface.

WHiSSPR refers to White Hat iDentity, Surveillance, Security, Privacy and Risk

- White Hat, referring to the ethical scheme of confidentiality as the report isn't designed to name and shame, but instead to effect the practices of the entities reported on.
- iDentity, refers to the focus of Personally Identifiable Information (PII), capturing, examining and mapping what identifiers are generated and the attributes they are linked to.
- Surveillance, refers to how the identifier's are used managed and shared, how many Controllers (often referred to as 3rd Parties, or Processors) the identifiers are shared with.
- Security, refers to the security of the PII, if PII is transferred internationally, if there is adequacy in the treatment and governance of the PII, and which party is the risk owner relative to the Controller responsible.
    - Every Controller the identifier is shared with, requires another WHiSSPR assessment, expanding scope of risk.
- Privacy, refers to the state of privacy, the legal justifications for processing and the scope of disclosure of the PII. Is it secure and encrypted on device? Is it in a cloud? How many parties are the identifiers exposed to
- Risk, is measured for each category out of a 100, rating the security risks of surveillance, the exposure, aggregation and scope of disclosure.
    - Rated out of a 100; where 1 is very low and 100 is very high privacy risk.

WHiSSPR utilises a identity industry, Data Controller Identity Record Schema[1] to generate a notice of the controller identity management practice, it applies the Kantara Initiative Transparency Performance Indiciators, to assess the performance of transparency to mitigate the risks, and how operational this transparency is to measure liability

Introduction

This WHiSSPR Report focuses on the proposed Canadian privacy legislation Bill C-27. The Canadian Consumer Privacy Act, the Canadian privacy legislation "to modernize privacy laws, enhance data protection, and introduce new regulations for AI."

It is presented as a Consumer Privacy Protection Act (CPPA) that is aimed at strengthening privacy protections and regulating how organizations handle personal data in Canada. This WHiSSPR report measures the transparency specified in this Bill to report on whether or not this legislation can deliver what it claims.

[1] Kantara Initiative, ANCR WG: Transparency Performance Scheme, v0.9 {online Sept 7, 2024]

In this report, the transparency and consent requirements in Bill C-27 are audited and compared against 4 legislative instruments, Quebec Law 25, the EU GDPR, and the international adequacy treaty Convention 108+, and the existing Candian Federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA).

Summary of Findings

This report reveals that, although the Bill C-27 is presented as a measure to modernize privacy legislation, it implements consumer protection practices, balanced against business surveillance interests. This results in deregulating privacy to allow third party surveillance of Canadians without transparency, permission or consent, making it very difficult to regulate the use of foreign surveillance in Canada.

Furthermore, this Bill instead of using standards, derrogates privacy in Canada by introducing a tribunal to adjudicate privacy law, rather than introducing the international Commonwealth treaty Convention 108+. This Bill is an indication of the dire need for policy that secures Canadian data sovereignty and implements privacy rights.

This WHISSPR report finds that in Bill C-27:

1. There are no requirements for the Controller Identity to be provided before asking for permissions to collect data
2. There is no mention of the legal justifications for processing personal data
3. Legitimate interest is introduced as a data surveillance tool for services and third parties, without requirements for permission or consent.

In conclusion, Bill C-27:

- Undermines national security, as it provides no protections against the surveillance of companies. Nor does it prevent secret surveillance practices by requiring records, logs or receipt requirements
- Does not modernise PIPEDA, as it violates the right to security in the Charter of rights and freedoms
- Derogates privacy as a right and Canada as. Culture of consent, to consumer protection rules, administered by terms and conditions, which do not implement security and or privacy people expect
- Creates a double standard as politicians are exempt from this privacy legislation.

This WHiSSPR Report analysis finds that the transparency requirements in Bill C-27 are not sufficient for international adequacy, there is no requirement for Controllers to create, or keep a record of surveillance processing activity, and no method presented to provide any type of operational accountability.
Without legally required transparency privacy regulation is not operationally effective to govern the use of surveillance.

Of notice, Bill C-27 introduces the concept of Consumer Privacy, which aims to balance the Citizens right to privacy against the interests of business and government. This is very similar to the approach taken in California Consumer Protection Act (CCPA) wherein 'consumers' must opt-in to privacy, and out of surveillance by default. In effect, removing barriers to the surveillance of citizens by foreign services, like the barriers put in place in the EU to address surveillance capitalism.

Bill C27 does not require foreign services to be transparent, to notify of surveillance, enabling large scale data scrapping and surveillance practices.

Unlike in the EU, there are no requirements for a record of processing activity when surveilling citizens. No requirement to notify or log surveillance and notice activities, no requirement for a data privacy officer, or regulator of surveillance practices. As a result Bill C27 is mis-leading in the requirements for consent, as consent requires citizens to be notified and informed of surveillance for consent to surveillance to be possible.

This Bill fails to even require the appointment of a data privacy officer or an accountable person to manage privacy and security risks.

Instead of rising to international standard practice of requiring a data privacy officer, Bill C-27 entrenches outdated privacy administration entrenching PIPEDA analogue privacy governance practices that it claims to modernise. Most notable, is the first country ever to propose the establishment of a politically led Tribunal to adjudicate privacy matters, rather than the implementation of security and privacy standards.

The Kantara Transparency Performance Indicators[2] are applied to evaluate the operational viability of transparency and consent as detailed in Bill C-27. This assessment quickly reveals that, while consent features prominently in the Bill, it lacks the required transparency for consent to be valid.

A high-level analysis of Bill C-27 reveals that rather than modernising privacy it aligns with the California legislation (CCPA), where consumers are required to opt-out of surveillance by default, placing the burden on the Individual to govern the data practices of services, not possible for children, accessible for the vulnerable, device or attention challenged individual. Relying on government and enterprise to self-regulate their data governance practices, which the FTC "makes clear that self-regulation has been a failure." America's hands-off approach has produced an enormous ecosystem of data extraction and targeting that takes place largely out of view to consumers."[3]

[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+an d+Conformity+Assessment+Scheme

[3] Financial Trade Commission (FTC) Sept 2024, [Internet] https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf

The most alarming of these is that Canadians' personal data and social profiles are predominantly hosted in American services, which do not afford privacy rights to non-US citizens and are subject secret surveillance and profiling by US security sercvice.

As a result, Canadians are without any explicit privacy or consumer protection.

Bill C-27 Analysis

Bill C-27 fails to meet Canadians' expectations for digital security and privacy, falling short of the protections guaranteed by Section 7 of the Charter of Rights and Freedoms[4], which includes protection from surveillance.

While the term 'consent' features prominently in this legislation, its transparency and accountability requirements are not sufficient for valid legal consent, are not compliant with Quebec Law 25, and is not adequate to international Commonwealth privacy treaty Convention 108+, which the GDPR mirrors. Importantly, there is no requirement to be transparency to be transparency about surveillance activities, to identify who controls the surveillance, or to maintain a log of surveillance processing, necessary to provide security and assurance that surveillance is governed and use for the specified purposes.

Clearly, a consumer protection framework that places business interests on par with the right to privacy results in inadequate privacy legislation that will not meet transborder data transfer, security, transparency and adequacy requirements. In addition, Bill C-27 is not compliant with Quebec Law 25[5], or the Canadian Supreme Court's R v Jarvis[6] decision on public privacy expectations.

This WHiSSPR report reports on critical security and governance concerns, to reveal negative impacts this legislation will inevitably have on Canadians, by downgrading privacy and subsequently security for personal data.

Impact Canadian Security an Identity Industry

Bill C-27's security and the authentication clauses work to deregulate the use of digital identity based surveillance technologies that profile individuals and online behaviours. This not only undermines the Pan-Canadian Trust Framework,[7] but also national and international security and privacy standards, which will enable wholesale data breach to the US and other foreign services.[8]

---

[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

[5] 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.

[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)

Part 1: Operational Transparency Audit

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 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.	The owner(s) or senior individuals in any organisation or institution, is accountable, mitigated by delegating this accountability to a data privacy officer (equivalent).
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 OECD11. 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.	

Table 1: Accountability

Bill C-27 Accountability - insufficient

In the GDPR and Convention 108+, which essentially mirror each other, there is a requirement (Article 13 and 14) to identify the Data Controlling organization and accountable person, as a minimum for accountable data processing. Bill C-27 has no such requirement to provide identity of Controller in Notice, notifications or disclosures for privacy, consent and surveillance.

Bill C-27 does not conform to standards, does not require a Record of Processing Activities (Article 30) and, as no Notice Receipt is required, does not require surveillance to be logged for legitimate interests (Article 88). A log provides security and assurance of compliance to existing regulation. This leaves legal consent in Canada, a global leader, in the digital dark ages.

Part 2: Openness and Transparency Audit

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
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.	

Table 2: Notice

Bill C-27 Openness and Transparency analysis

Bill C-27's Openness and Transparency Section 62 has only nine clauses. The most significant of these is clause 62(1), which is extremely vague.

The Bill only requires that organizations use plain language to explain the policies, without the requirement to identify the controller, or provide specific notice over confidentiality of processing, as required in Quebec.

In conclusion, this report recommends that transparency and consent be added to Bill C-27, and that a notice receipt, record or log be provided for all surveillance of personal data. This would put Canada back in the lead, and set the standard in the Commonwealth (2.5 billion people) for transparency and security with consent.

Bill C-27 requires significant revision, using standards and law, rather than a politicised regulatory process. This would make security and privacy in Canada operational.

Roles Terminology, Acronyms and References

These roles are mapped to the stakeholders involved. Although the names of these roles may vary across jurisdictions and languages, they correspond to roles requiring accountability as 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.

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 C-27

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

ANCR WG
Kantara Initiative: Anchored Notice and Consent Receipt Work Group focused on developing standards and best practices for managing and recording consent and notice in digital interactions.

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
- 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 and 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[9]
- 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 22, 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

[9] Digital Services Act came fully into force February 2024,

- 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[10]

- Convention 108+ Adequacy Baseline. ISO/IEC 29100 is interoperable with GDPR and Convention 108+ ,
- All of which is derived from the Conv 108, first signed in 1980, and the OECD 1980, Guidance for the Protection of in the Transborder Flows of Personal Information[11], 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.

[10] 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
[11] 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.


OPN
Digital Transparency Lab