NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

OHCHR Advisory Service on Digital Technologies Comments on Canadian draft Bill C-22 (the Lawful Access Act)
03 November 2026

Introduction

The Office of the United Nations High Commissioner for Human Rights (OHCHR/UN Human Rights) is the United Nations' leading human rights entity, mandated to document violations, contribute to international standards, and assess progress in protecting and promoting human rights worldwide.

This mandate extends to digital technologies. Under the United Nations Global Digital Compact, UN Human Rights advises stakeholders on aligning digital governance and regulation with international human rights norms and standards.

Further to requests to its OHCHR Human Rights Advisory Service on Digital Technologies offers selected comments on Bill C-22, "An Act Respecting Lawful Access," currently under debate in the Canadian Parliament. These non-exhaustive comments highlight key human rights questions in a spirit of constructive engagement, supporting alignment of Canada's regulatory efforts with international human rights law.

OHCHR notes that regulation of criminal investigative measures must comply with Canada's international human rights obligations, including the International Covenant on Civil and Political Rights (ICCPR), to which Canada acceded on 19 May 1976. Parts 1 and 2 of the Bill would significantly affect human rights, particularly the right to privacy (Article 17, ICCPR). As the Human Rights Committee emphasized in its review of Canada,[1] surveillance legislation must comply with Article 17 ICCPR and the principles of legality, proportionality, necessity and transparency, with effective safeguards including judicial review, independent oversight and adequate remedies.[2] OHCHR appreciates the emphasis on lawfulness in the Bill's title. As the Human Rights Committee and UN Special Procedures have observed, interference with privacy may nonetheless be unlawful where the underlying law does not comply with the Covenant's provisions, aims and objectives. The analysis below offers guidance on the conditions and safeguards needed to meet this standard.

[1] See CCPR/C/CAN/CO/7, paras. 45 and 46.
[2] See CCPR/C/CAN/CO/7, para. 46.

Structure of the Bill

Bill C-22, 'the Lawful Access Act' consists of three parts: Part 1 (Timely Access to Data and Information) which introduces amendments to the Criminal Code and to the Canadian Security Intelligence Service Act and other existing Acts; Part 2 (Supporting Authorized Access to Information Act) which introduces a new act; and Part 3 (Parliamentary Review).

Part 1 includes amendments to, amongst others, the Criminal Code and would govern law enforcement access to personal information held by communication service providers and technology companies and services. Part 2 enacts the Supporting Authorized Access to Information Act which would create a framework to respond to criminal activity in the digital space by expanding the authorities' powers of search and seizure, establishing the rules for what investigators may collect and compel from electronic service providers.

Analysis

I. Lawful Interference under the International Covenant on Civil and Political Rights (ICCPR)

Surveillance & Government Access via Intermediaries

Part 2 of Bill C-22, the Supporting Authorized Access to Information Act (SAAIA) raises significant concerns regarding lawful interference with the right to privacy. The draft permits Ministerial orders imposing obligations on core providers and a permanent duty to assist in assessing or testing devices, equipment or other means of authorized information access.[3] It is of particular concern that such requirements are proposed to be issued via Ministerial Orders subject to presumptive secrecy and without judicial authorization. Although Ministerial Orders are subject to the review of the Intelligence Commissioner,[4] the Intelligence Commissioner's Office has limited scope, and does not provide the necessary safeguards proportionate to how intrusive the proposed measures could be. Bill C-22 also prohibits the disclosure of certain government orders, raising transparency concerns. [5] Such intrusive surveillance should include independent prior authorization, subsequent audit and public disclosure. The UN General Assembly and Special Rapporteur on freedom of opinion and expression have emphasized non-arbitrariness, independent oversight and

[3] See Bill C-22, Part Articles 7, 5(2), and 13(1).
[4] See A/HRC/39/29, para. 39. on judicial review "[o]versight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated [...] Oversight processes must also be transparent and subject to appropriate public scrutiny, and the decisions of the oversight bodies must be subject to appeal or independent review."
[5] See Bill C-22, Part 2, Articles 14(c), 6(1) and 7(1).

redress in surveillance legislation.[6] The Human Rights Committee has noted that interference may still be considered arbitrary, even when provided for by law,[7] and that "reasonableness" means that any interference with privacy must be both necessary and proportionate to the end sought within the circumstances of the particular case.[8] Here, the Bill permits the Minister to deny disclosure on "reasonable" grounds without defined limits (which would clarify how such measures are necessary and proportionate) or a duty to publish their reasons for the disclosure's denial.[9] As the Human Rights Committee has noted, excessive executive discretion lacks the necessary qualities of law as secrecy compounds the risk of arbitrariness.[10] Without safeguards, these provisions do not meet international law's non-arbitrariness requirements.

Additionally, Article 5(2) gives the government the authority to obligate providers to create pathways for an authorized person to access information. Article 20 allows the government to designate any person to enter private property and access computer data without a warrant. The combination of these two articles, coupled with broad data retention obligations, creates instances where the government could effectively bypass the service provider to access information directly. Under the United Nations Guiding Principles on Business and Human Rights (UNGPs), electronic service providers retain an independent responsibility to respect human rights, including when responding to government demands for access to information.[11] This responsibility supports scrutinizing and, where appropriate, challenging demands that would result in adverse human rights impacts. Provisions allowing public authorities to bypass providers may impede providers ability to assess such demands and take appropriate action to prevent or mitigate those impacts.

II. Search & Seizure

As outlined above, the Bill would enact the Supporting Authorized Access to Information Act, expanding search and seizure powers to address digital crime and defining what investigators may collect and compel from electronic service providers.

Seizures must comply with legality, necessity, and proportionality under international human rights law. The broad terms in the Bill such as "exigent circumstances" and "impracticable"[12] risk

[6] See A/RES/77/211 and A/HRC/34/61, para. 36.
[7] See A/HRC/27/37, para. 21.
[8] Ibid.
[9] See Bill C-22, Part 2, Articles 15(1) and 14.
[10] See A/HRC/27/37, para. 29.
[11] Principle 23(b), read together with Principle 11, calls on enterprises to seek ways to honour internationally recognized human rights when faced with conflicting domestic requirements.
[12] Bill C-22, Part 1, Article 487.11.

permitting seizures without judicial oversight, while authorization to seize "any subscriber information" lacks clear limits on scope, justification and duration. Given readily accessible emergency warrants under Canadian federal criminal law, including remote requests approved within hours, OHCHR strongly recommends safeguards ensuring legitimate and proportionate search and seizure and preventing indefinite, arbitrary retention of data or property. Leaving these decisions to law enforcement at seizure risks unlawful and arbitrary interference with privacy of correspondence and freedom of expression under ICCPR Articles 17 and 19, respectively.

Under ICCPR Article 17, the Human Rights Committee has found property seizures and data collection unlawful where it was disproportionate to the alleged threat and where the specific data collected could not be ascertained. Lawful data access requires identifiable, non-arbitrary reasons and effective remedies for search and seizure. OHCHR would like to draw attention to the lack of adequate precision in certain Canadian Criminal Code terms, such as "building" and "place,"[13] which Canadian Courts have already highlighted lack sufficient particularity.[14]

This reflects ICCPR Article 17's requirement that domestic law specify in detail the circumstances in which search warrants may apply.[15] The same applies to "computers,"[16] which may hold considerable personal data unrelated to a suspect. Prior authorization for the specific search is therefore necessary to respect proportionality. OHCHR recommends that the amendments require greater precision regarding locations and computers, and that Article 487(2.5) be edited accordingly.

Article 20(3) authorizes persons designated under Article 20(1) to examine anything on the premises, copy documents and electronic data, remove documents, and use computers and copying equipment, while Article 20(5) requires everyone present to assist. These powers lack judicial review or independent oversight, which represents a significant risk of arbitrary and disproportionate interference with the right to privacy under Article 17 of the ICCPR.

Warrants

Article 487(2.4) (a) risks overly broad discretion by permitting computer data and system search warrants on the belief that an offence "will be committed." It should specify precise grounds linked to concrete conduct and intent, rather than speculative future danger, and require case-by-case

[13] See Bill C-22, Part 1, Article 487(2.1).
[14] See *R v Vu*, 2013 SCC 60.
[15] See Bill C-22, Part 1, Article 487(1).
[16] See Bill C-22, Part 1, Article 487(2.4).

judicial assessment to prevent arbitrary interference with privacy.[17] Under human rights law, warrants require case-by-case authorization by an authority designated by law and must pursue a legitimate aim.[18] Information obtained during the process of the warrant should only include what is necessary to the investigation and must not amount to harassment.[19] The principles of necessity and proportionality require time-limited authorizations, renewal only on fresh justification and discontinuation of the warrant when no longer necessary.[20] OHCHR is concerned that Article 487(2.8) does not meet this threshold. Individuals should be notified of surveillance once notification no longer jeopardizes its purpose, enabling access to remedies. Restrictions or delays must be strictly limited.[21]

III. Indiscriminate Metadata Retention and the Right to Privacy

Data collection interferes with the right to privacy.[22] The right to privacy protects both communications content and metadata, which, when aggregated and analyzed, may reveal "an individual's behavior, social relationship, private preference, and identity that go beyond even that conveyed by accessing the content of a communication."[23] Data collection and use require "clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."[24] OHCHR recommends adding safeguards into Article 487(2.8) ensuring warrant extensions meet necessity requirements under international human rights law. References to data types remain vague throughout the draft, including "transmission data" broadly relating "to any means of telecommunication that is unknown at the time the warrant is issued."

Mandatory, indiscriminate metadata retention by telecommunications companies and electronic service providers interfere with privacy, limits anonymous communication, risks abuse and third-party disclosure,[25] and exceeds necessity and proportionality. Article 5(2) permits such retention without requiring that data be liable to give rise to criminal prosecution or necessary to

[17] See CCPR/C/GC/16.
[18] See CCPR/C/GC/16, para. 8.
[19] Ibid.
[20] See A/HRC/27/37, para. 28 and A/HRC/39/29.
[21] See A/HRC/27/37, para. 47 and A/HRC/23/40, para. 82.
[22] See A/HRC/27/37, para. 20.
[23] See A/HRC/27/37, para. 19.
[24] *Podchasov v Russia*, App No 33696/19, Judgment, European Court of Human Rights (13 February 2024).
[25] See A/HRC/39/29, para. 18.

address national security threats.[26] This raises serious concerns about a surveillance regime retaining transmission and location data without specifying the offence under investigation, establishing necessity for a specific criminal investigation or national security threat, or the proportionality of the surveillance. The absence of judicial authorization, independent review and notification further risks that secret retention orders will evade effective challenge.

IV. Critical Technical Safeguards

Bill C-22 threatens to undermine end-to-end encryption and disproportionately infringe upon the right to privacy. The Bill proposes broad facilitation of access obligations, plus the future possibility of introducing regulations[27] to further impose technical monitoring capacities. OHCHR welcomes that Article 5(5) would exempt core providers from requests introducing a "systemic vulnerability," understood as intended to safeguard end-to-end encryption. In practice, however, obligations under Articles 2(4), 5(2) and 7(1) are very difficult, if not impossible, to meet without introducing such vulnerabilities. OHCHR consistently emphasizes strong encryption as essential to privacy, online security and safeguarding rights, and suggests an explicit clause: "*nothing in this law should be understood as compelling service providers to break critical technical safeguards, such as end-to-end encryption.*"

OHCHR has noted that "the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the targeted individuals but the general population."[28] The Committee also raised concerns that Bill C-8, amending the Telecommunications Act, would permit government access to sensitive data without prior judicial authorization or key safeguards on the data obtained, and could compel companies to break critical technical safeguards such as encryption.[29]

V. Cross-border data sharing

Bill C-22 expands cross-border data-sharing conditions, including mutual legal assistance (Article 29, 22.07(3), 487.0142). It appears to lower the threshold for law enforcement access to subscriber information from a reasonable belief standard to a reasonable suspicion standard, requiring only that "there are reasonable grounds to suspect that" information would "assist" an investigation—a low, easily met relevance standard.[30] Access and sharing interfere with privacy;

[26] See Bill C-22, Part 2, Article 5(2).
[27] See Bill C-22, Part 2, Article 5(2).
[28] See A/HRC/51/17.
[29] See CCPR/C/CAN/CO/7, para. 45.
[30] See Bill C-22, Article 487.0142(2).

these thresholds may therefore weaken its protection in cross-border requests. International human rights law requires prior independent judicial review of necessity and proportionality to prevent arbitrary interference. The lack of this safeguard and apparent absence of data minimization obligations increases the risk of arbitrary and unlawful interference in practice.

OHCHR recognizes the often-legitimate need for cross-border data sharing in criminal investigations. Global experience nonetheless shows its recurring use outside of such investigations for offences that should not be criminalized under international law, or for transnational repression.[31] A legal framework must therefore clearly define when and how sharing may occur and minimize abuse. Given growing data-enabled transnational repression, the law should require dual criminality and rejection of requests where reasonable grounds indicate that sharing will result in serious human rights violations. Without these safeguards, Canada's legal framework risks enabling persecution of individuals, including human rights defenders and journalists, in other States.

Concerns about provisions empowering or compelling Canadian service providers to send transmission data, subscriber information or other personal information to foreign States are heightened by the absence of access to remedies for resulting human rights violations. OHCHR strongly recommends reviewing the Bill's cross-border data-sharing provisions to establish further conditions ensuring compliance with international human rights law.

ENDS/

[31] See A/HRC/56/53.