

**Privacy Regulation Roundup – January 2024**

This Privacy Regulation Roundup summarizes the latest major global privacy regulatory developments, announcements, and changes. This report is updated on a monthly basis. For each relevant regulatory activity, you can find actionable Info-Tech analyst insights and links to useful Info-Tech research that can assist you with becoming compliant.

Contents

[Canadian Government Under Review for Digital Surveillance Technology Use 3](#_Toc156545381)

[Type: News 3](#_Toc156545382)

[Date: November 29, 2023 3](#_Toc156545383)

[FTC Proposes Strengthening COPPA to Bolster Privacy Safeguards for Children 4](#_Toc156545384)

[Type: Regulations 4](#_Toc156545385)

[Announcement Date: January 2024 4](#_Toc156545386)

[ICO’s Guidance on Risk Assessments for UK-US Data Transfers 5](#_Toc156545387)

[Type: Guidance 5](#_Toc156545388)

[Date: December 2023 5](#_Toc156545389)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Canadian Government Under Review for Digital Surveillance Technology Use

## Type: News

## Date: November 29, 2023

**Summary:** ThirteenCanadian federal departments are facing criticism for using tools designed to extract personal information from end-user devices. The tools can recover and analyze data found on computers, tablets, and mobile phones, including encrypted and password-protected information. Shared Services Canada purchased the equipment and software for the government in 2023.

A directive from the Treasury Board of Canada Secretariat (TBS) requires that all federal institutions carry out a privacy impact assessment (PIA) before implementing activities that involve the collection or handling of personal information. The goal of a PIA is to identify and mitigate privacy risks. In this case, none of the departments using the software carried out a privacy impact assessment.

Some departments claimed a PIA wasn’t necessary because they already had judicial authorizations that impose strict conditions on the seizure of electronic devices. Others said they only used the material on government-owned devices, for instance, in cases involving suspected fraud or harassment. According to Canada’s Privacy Commissioner, Philippe Dufresne, however, a judicial authorization does not remove the requirement to conduct a PIA.

A parliamentary committee will study the use of digital surveillance tools within the federal government in January 2023.

**Analyst Perspective:** The responsibility for conducting a PIA typically lies with the entity initiating a new project or policy, or making changes to existing processes that involve the collection, use, or handling of personal information. In this case, federal government departments deploying the technology are in the best position to understand the specifics of the data handling involved and assess potential privacy impacts. In contrast, the shared services organization that provides the tool is responsible for ensuring the tool itself has baseline privacy safeguards and complies with relevant privacy laws.

Under Canadian privacy legislation, government departments are responsible for conducting PIAs for all new programs and services that raise privacy issues. This is in accordance with the “Directive on Privacy Impact Assessment” from the Treasure Board of Canada Secretariat. The PIA goes through an internal approval process before the Deputy Minister approves it and sends it to the Office of the Privacy Commissioner for review.

The case illustrates the need to implement robust governance measures when building a privacy program and maturing privacy operations and then to audit these measures regularly.

**Analyst:** [Michel Hébert](https://www.infotech.com/profiles/michel-hebert), Principal Research Director – Security & Privacy

**More Reading:**

* Source Material: [CBC](https://www.cbc.ca/news/canada/ottawa/federal-canada-government-department-privacy-1.7041255), [CBC](https://www.cbc.ca/news/canada/ottawa/data-extraction-federal-canada-government-committee-report-1.7051043?mkt_tok=MTM4LUVaTS0wNDIAAAGP6XKtdC6ofVv4SNYjxc8_RalAeziL2N9DhLfqxl9ft8krpyriEk8nDgi3eUTKdrm4nBSeB0gmPUa8nK-OMHjc_SsMFLZw9W9q-DWbopdp0MdB), [Government of Canada](https://www.canada.ca/en/health-canada/corporate/about-health-canada/activities-responsibilities/access-information-privacy/privacy.html), [OPCC](https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/02_05_d_33/), [TBC](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308)
* Related Info-Tech Research:
  + *[Mature Your Privacy Operations](https://www.infotech.com/research/ss/mature-your-privacy-operations)*
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# FTC Proposes Strengthening COPPA to Bolster Privacy Safeguards for Children

## Type: Regulation

## Announcement Date: January 2024

**Summary:** In a bold move to recalibrate the digital landscape for children, the Federal Trade Commission (FTC) has proposed significant amendments to the Children’s Online Privacy Protection Act (COPPA). These revisions target the tracking and hoarding of children’s personal data by imposing stricter controls over data collection, disclosure, and monetization practices. The current COPPA framework hinges on parental consent for data collection from children under 13. However, some argue that this onus alone proves insufficient in the face of sophisticated digital tools deployed to surveil children today online.

Rather than relying solely on parental gatekeeping, the FTC envisions affirmative obligations on service providers. This translates to limitations on the types and volume of data collected, stricter retention guidelines, and robust data security measures. Importantly, the FTC proposes to curtail the commercial exploitation of children’s data altogether. This is a move that seeks to ensure that children play and learn online free from such risks.

The FTC’s proposed amendments extend their reach beyond data collection, targeting the tools used to engage children online. There is a proposed ban on “persistent identifiers” – digital markers that track online activity – without parental consent. Operators relying on this exception would face transparency requirements and be forced to explain operations and demonstrate how these identifiers won’t be used for targeted advertising or directly contacting children.

Furthermore, the FTC seeks to curb the use of information gathered under COPPA exceptions to send push notifications that incentivize increased website engagement. This aims to address concerns about websites exploiting loopholes that encourage children to increase usage, potentially at the expense of their wellbeing. Data retention also faces stricter scrutiny. The FTC proposes allowing operators to hold children’s data only as long as necessary, effectively prohibiting its use for secondary purposes beyond the initial reason for collection. This aligns with the goal of minimizing data exposure and mitigating potential harm.

To bolster data security, the FTC mandates the creation of formal programs surrounding children’s personal information security. These programs would serve as blueprints for safeguarding sensitive data, ensuring there are safeguards in place appropriate to the sensitivity of the information collected. The FTC encourages public participation, inviting comments on the proposed changes within 60 days of publication in the Federal Register, this shines a light on the open dialogue and collaborative approach the FTC is committed to.

**Analyst Perspective:** The proposed FTC regulations on children’s online privacy have garnered strong support from advocates who see them as a critical step toward a safer online environment for children. The recent FTC actions against tech giants like Meta further demonstrate the need for robust regulations, especially in light of Meta’s resistance and claims of political motivations. This call to action underscores the collective responsibility to create a digital environment that ensures children are safe and fosters healthy online interactions.

**Analyst**:[Carlos Rivera](https://www.infotech.com/profiles/carlos-rivera), Principal Advisory Director – Security, Privacy, Risk & Compliance

**More Reading:**

* Source Material: [FTC](https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens), [NY Times](https://www.nytimes.com/2023/12/20/technology/ftc-regulation-children-online-privacy.html), [Engadget](https://www.engadget.com/the-ftc-wants-to-strengthen-coppa-to-make-it-harder-for-companies-to-monetize-kids-data-214459097.html)
* Related Info-Tech Research:
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# ICO’s Guidance on Risk Assessments for UK-US Data Transfers

## Type: Guidance

## Date: December 2023

**Summary:** Following the Schrems II case in 2020, Transfer Risk Assessments (TRAs) are now mandatory for organizations engaged in restricted transfers of personal data to the United States under Article 46 of the UK GDPR. To that end, the Information Commissioner’s Office (ICO) has released updated guidance TRAs.

A TRA is a comprehensive risk assessment ensuring that the chosen Article 46 mechanism effectively safeguards against risks to individuals’ rights in the destination country. This includes risks from third-party access and challenges in enforcing the transfer mechanism.

The ICO’s new guidance encourages organizations to integrate the Department for Science, Innovation, and Technology (DSIT)’s published analysis in the organization’s TRA to streamline the process for UK-US transfers. The analysis covers critical aspects such as the rule of law, fundamental rights, supervisory authority, and relevant US laws and practices. The guidance aims to provide a practical approach to addressing complexities while ensuring ongoing compliance with evolving regulatory landscapes.

**Analyst Perspective:** Understanding the intricacies and expenses tied to TRAs, the ICO’s latest guidance proposes an efficient approach for organizations to leverage DSIT’s analysis by reference. This will reduce duplication of the analysis process in managing risks linked to third-party access and complexities related to enforcement.

Organizations can now use practical examples provided by the ICO that demonstrate how organizations can apply the DSIT analysis in real-world scenarios, aligning it with specific transfer mechanisms like the International Data Transfer Agreement or the UK Addendum to the Standard Contractual Clauses. This not only streamlines the compliance process but also provides a tangible framework for implementation.

While the guidance endeavors to alleviate the compliance burden, it crucially underscores the ongoing responsibility of organizations to maintain vigilance. Regular review of any updates to the DSIT analysis is emphasized. If there are alterations in DSIT’s conclusions, organizations are advised to promptly reassess and update their TRAs, ensuring that their data transfer practices remain in harmony with evolving regulatory dynamics. This strategic guidance serves as a practical roadmap for organizations navigating the intricate terrain of data transfers, aiming to balance compliance efficiency with the evolving landscape of data protection regulations.

**Analyst:** [Safayat Moahamad](https://www.infotech.com/profiles/safayat-moahamad), Research Director – Security & Privacy

**More Reading:**

* Source Material: [UK ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/international-data-transfer-agreement-and-guidance/transferring-personal-information-to-the-us/), [IAPP](https://iapp.org/news/a/ico-issues-transfer-risk-assessment-guidance-for-us-transactions/)
* Related Info-Tech Research:
* [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)