Blaney McMurtry LLP

PUBLICATION

New Tool Introduced by the OPC Helps Organizations Assess Real Risk of Significant Harm

Date: July 21, 2025
Author: Angelique Bedford

INTRODUCTION

On March 26, 2025, the Office of the Privacy Commissioner of Canada (the "OPC") introduced the Real Risk of Significant Harm Assessment Tool (the "Tool") to help organizations determine whether a privacy breach meets the real risk of significant harm reporting threshold under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). This Tool represents a critical step forward in operationalizing the OPC's legal guidance and turning it into a more practical, structured framework.

PIPEDA BREACH REPORTING OBLIGATIONS

PIPEDA is Canada's federal privacy law for private-sector organizations. It sets out ground rules for how businesses must handle the collection, use and disclosure of personal information during commercial activity. Since amendments of PIPEDA came into force in November 2018, organizations are required to report to the OPC and notify affected individuals of certain breaches involving their personal information.

Specifically, pursuant to section 10.1 of PIPEDA, organizations must notify the OPC and affected individuals of a breach of security safeguards involving personal information under the organization's control where the breach poses a "real risk of significant harm". Such provisions aim to promote greater transparency and accountability, while allowing individuals to take steps to protect their personal information.

WHAT IS A "REAL RISK OF SIGNIFICANT HARM"?

PIPEDA requires reporting when it is reasonable to believe that a breach of security safeguards creates a real risk of significant harm ("RROSH") to the individual.

PIPEDA's definition of "significant harm" is intentionally broad, encompassing bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or

loss of property. The threshold is not minimal – there must be a real and significant possibility of harm, not a speculative or theoretical one.

In such cases where a breach creates a RROSH, an organization must:

1. report the breach to the OPC by submitting a breach report form through the OPC's website;
2. notify affected individuals directly by telephone, mail, email, or any other form of communication that a reasonable person would consider appropriate in the circumstances; and
3. maintain a record of every breach for 24 months, regardless of whether it meets the threshold for reporting.

WHEN DOES A RROSH EXIST AND HOW TO ASSESS?

Relevant factors in determining whether a breach of security safeguards creates a RROSH include:

1. the **sensitivity** of the personal information involved;

- This is assessed in context. For example, even contact information could be considered sensitive if it is associated with other personal identifiers or if its disclosure could expose someone to harm.

2. the **probability** that it has been, is being, or will be misused; and

- Probability of misuse depends on circumstances such as the nature of the breach, the intent and capability of the threat actor, whether the data was encrypted or anonymized, and if the breached data has been recovered.

3. any other **prescribed factor**.

- As of the date of this publication, no additional factors have been prescribed.

While this framework provides helpful direction, the guidance leaves room for interpretation, which has led to inconsistency and uncertainty among organizations seeking to comply with PIPEDA.

THE NEW TOOL

To help businesses assess a RROSH to an individual, the OPC introduced the Tool.

What is the Tool?

The OPC's new assessment Tool is designed to support organizations in determining whether a privacy breach is likely to result in a RROSH to individuals and, consequently, whether breach reporting obligations under PIPEDA are triggered. It takes the form of a user-friendly, fillable questionnaire that systematically guides organizations through the core factors they must

consider under PIPEDA. Notably, the Tool does not request any identifying information about the organization using it, and no data entered is collected or transmitted to the OPC.

The Tool's design not only helps ensure that key factors are considered in a consistent manner, but also supports internal governance, regulatory transparency, and risk mitigation. By prompting organizations to document their rationale for reporting decisions, the Tool could also serve as valuable evidence in the event of an OPC investigation.

How to use it?

To effectively use the Tool, organizations must first identify the types of personal information involved in the breach (e.g., contact details, demographic data, banking information, government-issued identification, communications, surveillance data, or health records) and estimate the number of individuals affected.

The Tool guides users through a series of contextual questions concerning the breach based on previous answers. These include how the incident occurred, who received the exposed information, the relationship between the recipient and the affected individuals, and whether the individuals may possess characteristics that heighten their vulnerability (e.g., unfamiliarity with Canadian laws, a criminal record, involvement in legal or custody disputes, or existing personal safety risks).

Once the responses have been submitted, the Tool generates a report indicating whether the breach is likely to meet the RROSH threshold and if reporting is required. Additionally, the report highlights potential associated harms such as financial fraud, phishing attempts, reputational harm, exploitation, or identity theft.

It is important to note that the Tool is specifically designed to support compliance with privacy breach notification obligations under PIPEDA. Organizations may be subject to additional breach reporting requirements under other legal frameworks, depending on their jurisdiction, the nature of the information systems involved, and the location or status of affected individuals. As such, organizations are strongly advised to consult with their privacy and legal teams to ensure that all applicable obligations are identified and addressed.

It is also crucial to keep in mind that the Tool is not a substitute for an organization's formal risk assessment process or for obtaining legal advice. Certain factors relevant to a comprehensive risk analysis may fall outside the scope of the tool, while other elements may receive disproportionate weight due to a lack of broader context. Accordingly, the Tool should be viewed as a helpful preliminary resource to guide an organization's RROSH analysis by identifying key questions and considerations, but its results should not be treated as definitive.

What impact will the Tool have in future?

Looking ahead, organizations that use the Tool thoughtfully and consistently may benefit from increased regulatory credibility. While voluntary, the Tool reflects the OPC's evolving

expectations and may become an informal benchmark for compliance in future investigations or audits.

If you have any questions about the new Tool, how PIPEDA applies to your organization, or whether you are in compliance with the applicable laws, please reach out to the author.

The author would like to acknowledge and thank articling student, Callum Paleczny, for his contributions to this article.