Digital marketing and analytics: Lessons for Canadian retailers using offline conversion tools following Privacy Commissioner's ruling

February 20, 2023

A recent decision by the Office of the Privacy Commissioner of Canada (OPC) illustrates the complex and often ambiguous nature of consent under Canadian federal privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). It also highlights key implications for Canadian retailers processing data as part of their digital marketing and analytics efforts, using offline conversion tools.

Background

In PIPEDA Findings # 2023-001, these issues are discussed in the context of a complaint related to the sharing of customers' personal information by a Canadian retailer, Home Depot of Canada Inc., with Facebook's parent company, Meta Platforms, Inc. (f/k/a Facebook, Inc.) (Meta), using its business tool known as "Offline Conversions." This tool helps businesses measure the impact of their online advertising campaigns on in-store sales by sharing a hashed version of their customers' contact information and in-store transaction data with a third-party platform, which matches the information to users of the platform and compares the transaction data to the ads shown to those users. This enables businesses to make informed decisions about ad spending and improve their digital marketing strategy.

In concluding that an opt-in form of consent was required, the OPC relied on its determination that the data-sharing situation with the social-networking platform fell outside the reasonable expectations of customers who provided their email addresses to receive e-receipts. This conclusion was reached even though the practice did not involve any sensitive personal information or pose an immediate risk of significant harm to customers.

In addition, the OPC held that customers should have been actively informed of key elements related to the data-sharing practice at the time of collection, including the fact that the social-networking platform was contractually permitted to use the information for its own business purposes. This underscores the risks associated with relying solely on information contained in a privacy policy to obtain meaningful consent for secondary marketing and analytics purposes.

This decision highlights some of the grey zones under Canadian privacy laws and the challenges that businesses face in interpreting and applying the notion of consent and the "reasonable expectations" standard. In fact, media reports following the release of this decision highlighted the fact that many other major Canadian retailers may have also been using Meta's Offline Conversions tool without obtaining opt-in consent from customers, illustrating that other industry players were interpreting these legal grey zones in a similar fashion.

The above underscores the need for a more collaborative approach between the industry and Canadian privacy regulators to better understand the marketing and analytics practices and needs of businesses, and to proactively develop clear, practical guidance on how to implement these practices in compliance with Canadian privacy laws.

While the decision does not preclude organizations from relying on implied consent for all forms of marketing and analytics, it does bring to light the importance of providing individuals with upfront notice of such practices, placing clear limits on partners' use of the information, and making it easy and convenient for individuals to withdraw their consent for secondary purposes. However, the lack of clear regulatory guidance on these issues means in turn that organizations that rely on an opt-out form of consent to process information for marketing and analytics will always face a risk of non-compliance, particularly for novel practices that may arguably fall outside of individuals' reasonable expectations.

Privacy considerations related to the use of offline conversion tools

1. Distinction between "use" and "disclosure" of personal information when information is shared with a third-party analytics partner

Under PIPEDA, sharing personal information with a service provider is considered a "use" of personal information rather than a "disclosure." This means that an organization that has obtained valid consent to collect and use personal information for specific purposes may share that information with a service provider without having to obtain additional consent, provided that the service provider processes the information only for those purposes.[1] Both the service provider and the organization that retains its services to process personal information on behalf of the organization have obligations under PIPEDA to protect the information and to ensure that the information is processed only for the purposes for which consent was obtained.[2]

The OPC in this case reviewed the agreement between the retailer and the social networking platform and concluded that the platform was acting more than just as a service provider, but rather as an independent organization processing the information for its own business purposes, including targeted advertising. As a result, the OPC articulated the view that the sharing of customers' personal information with the third party was a "disclosure" rather than a "use" of that information, triggering the need for additional consent.

2. The form of consent and its relationship to the reasonable expectations of individuals

The OPC's Guidelines for Obtaining Meaningful Consent recognize that the form of consent will vary depending on the circumstances and the type of information collected. In general, express consent is required when a processing activity (i) involves sensitive personal information, (ii) falls outside the reasonable expectations of individuals, *or* (iii) creates a significant residual risk of significant harm. This means that even if personal information is considered "less sensitive," opt-in consent may still be required where the processing activity for which consent is sought falls outside the reasonable expectations of individuals.[3] This raises the question of how to determine what constitutes "reasonable expectations" in a given context, particularly where the information is non-sensitive and is processed for purposes that serve the legitimate business interests of an organization, such as measuring the performance of its digital marketing campaigns.

"Reasonable expectations" is an objective standard that requires consideration of "all of the relevant contextual factors surrounding the practice in question, including the type of services the organization offers, and the nature of the relationship between the organization and its customers. These contextual factors must not be considered in isolation but rather, evaluated as a whole."[4] In *Royal Bank of Canada v. Trang*, the Supreme Court of Canada favoured a broad interpretation of this standard, one that requires an examination of "the whole context," including the relationship between the individual whose information is being disclosed and the third party to whom the organization is disclosing the information, the identity of that third party, and the purpose for seeking disclosure.[5] To do otherwise, the Court continued, "would unduly prioritize privacy interests over the legitimate business concerns that PIPEDA was also designed to reflect."[6]

The OPC's analysis of the "reasonable expectations" issue is as sparse as it is ambiguous, leaving much room for speculation about the broader implications of the decision for other common marketing and analytics practices, such as targeted advertising. While acknowledging that the information was not particularly sensitive in the context of this case, as the transaction information shared identified only the department in which a purchase was made and not the actual product purchased, the OPC nonetheless concluded that opt-in consent was required to share information to measure offline conversions, since customers who request an e-receipt in-store would not "reasonably expect, or have any reason to suspect," that their personal information would be shared with a third party to measure the effectiveness of its online advertising campaigns or for the third party's own business purposes.

However, this reasoning may conflate two distinct issues: the form of consent, and compliance with notice and transparency requirements. This raises the question of whether, and if so to what extent, notice and transparency can help shape the reasonable expectations of individuals so that implied consent would become appropriate in the circumstances. While the OPC's findings and recommendations seem to preclude this option, the fact that the form of consent analysis appears to incorporate the issue of transparency leaves open the possibility that a different result on the form of consent issue might have been reached if there had simply been more transparency in the first place.

It is important to acknowledge that the decision did not explicitly consider the practical implications of requesting an opt-in form of consent at the time a customer makes an in-store purchase, nor the presence of countervailing factors in determining the reasonable expectations of customers. Such factors may include the legitimate business interests at play, the pre-existing relationship between the social networking platform and the customer, and the ability to control how the social-networking platform processes offline event data through a user's account settings. For example, could it not be said that users of the platform have a different reasonable expectation than non-users, given their pre-existing relationship with the third party and the privacy notices and choices communicated to them through the platform? There are also the potential practical and technical challenges associated with implementing an opt-in form of consent in an offline environment, raising the question of whether it strikes the appropriate balance between privacy interests and business needs that PIPEDA seeks to protect.

While the answer to the above questions may ultimately depend on the nature and scope of the processing activities involved, the OPC missed an opportunity to explore these questions and clarify one of the murkier aspects of the notion of consent under PIPEDA, namely the "reasonable expectations" standard and its emerging role in determining the form of consent.

3. Notice and transparency requirements and their role in obtaining meaningful consent

Under PIPEDA, an organization must make reasonable efforts to inform individuals, before or at the time of collection, of the nature, purpose and consequences of the processing for which consent is sought, taking into account the individual's reasonable expectations.[7] According to the OPC's Guidelines for Obtaining Meaningful Consent, organizations should place additional emphasis up front on key elements of their information handling practices, such as the types of information collected, the entities with whom the information is shared, the purposes for which the information is processed, and the risks of harm and other consequences resulting from the processing activities.

Setting aside the "form of consent" issue, the OPC considered whether the retailer could rely on its privacy statement and Meta's privacy policy to inform customers of these practices. In concluding that these documents were not sufficient to obtain meaningful consent, the OPC held that the retailer should have provided a "just-in-time" notice to inform customers of the nature, purposes and consequences of the data-sharing with the social-networking platform.

What the decision means for businesses and cross-channel marketing and analytics

For businesses, the OPC's assessment of the "reasonable expectations" standard is likely to raise more questions than answers and will naturally lead many to wonder whether other common marketing and analytics practices, such as online behavioural advertising, retargeting, custom audiences and other forms of targeted advertising, may require opt-in consent and greater transparency at the time of collection. After all, there are many grey zones in Canadian privacy laws that make key concepts such as the form of consent difficult to apply in practice without clear regulatory guidance, thereby

increasing the risk that industry-wide practices, no matter how well established, could end up being deemed unlawful upon investigation by a privacy regulator.

In some cases, implied consent may still be acceptable when processing information for secondary purposes, provided that the facts surrounding a particular practice are sufficiently distinguishable from those mentioned in the OPC's recent decision. For example, the OPC has previously stated that an opt-out form of consent could be considered reasonable for online behavioural advertising (OBA) subject to certain conditions detailed in its Guidelines and Policy Position paper.[8] While this raises the thorny question of whether it can truly be said that users reasonably expect that their online-browsing data will be used to deliver targeted ads, it is unlikely that this decision, which only involved data sharing for the purpose of measuring the impact of the retailer's digital marketing campaigns on in-store sales, was intended to change the status quo regarding the form of consent required in the context of OBA. However, organizations should pay close attention to the measures they put in place to ensure that they are sufficiently transparent at the point of collection, limit how partners can use the information, and provide an easily accessible and convenient means for individuals to withdraw their consent for secondary purposes.

Business takeaways

Despite some lingering questions about the broader implications of the OPC's recent decision on cross-channel marketing and analytics, organizations should consider working with their marketing teams to review their use of offline conversion tools and other secondary practices involving the collection and processing of personal information to assess compliance with Canadian privacy laws.

Depending on the context, organizations may also want to take certain steps to improve compliance with these laws, including:

- Identifying which marketing and analytics tools or practices are used and how information is collected, used, or disclosed in connection with those tools or practices, including any data sharing with third parties;
- Reviewing consent flows to verify and confirm that the form of consent obtained is appropriate in light of the sensitivity of the information and the reasonable expectations of individuals;
- Providing individuals with a "just-in-time notice" that contains key information about the practices for which consent is being sought at the time of collection;
- Updating the language used in privacy communications to improve clarity and provide a greater level of detail about specific marketing and analytics activities; and
- Reviewing agreements with third-party platforms and analytics partners to verify the limits placed on their use and disclosure of personal information and, where appropriate, updating privacy notices and consent language to accurately reflect any disclosures of personal information to third parties for their own business purposes.

Ultimately, the OPC's recent decision regarding the use of offline conversion tools has highlighted the urgent need for greater collaboration between industry and Canadian privacy regulators. It is crucial that the industry is not caught off-guard by the interpretation of key privacy concepts such as the notion of consent, particularly in the

areas of marketing and analytics, which are critical components of many organizations' business models. Organizations need practical guidance and compliance tools that provide certainty and predictability in the application of these legal requirements. The risks of non-compliance can be significant, including reputational harm and potential financial liabilities, particularly under federal and provincial privacy law reforms. A more proactive, collaborative approach is therefore essential to protect customers and support businesses.

Footnotes

[1] For example, see PIPEDA Findings #2019-004, paras. 17-20; PIPEDA Findings #2020-001, para. 22.

[2] For example, see PIPEDA Findings #2022-001, para. 83; PIPEDA Findings #2019-004, para. 66.

[3] PIPEDA Report of Findings #2015-001, para. 77.

[4] PIPEDA Report of Findings #2015-001, para. 78.

[5] *Royal Bank of Canada v. Trang*, [2016] 2 SCR 412, paras. 43-46.

[6] *Royal Bank of Canada v. Trang*, [2016] 2 SCR 412, para. 44.

[7] Section 6.1 and Principles 4.3.2 and 4.3.5, PIPEDA.

[8] See also PIPEDA Report of Findings # 2013-017; PIPEDA Report of Findings #2014-001; PIPEDA Report of Findings #2015-001.

By

Andy Nagy

Expertise

Cybersecurity, Privacy & Data Protection, Information Technology, Online Retail & E-commerce

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749