Goodmans LLP Update

Privacy Commissioner of Canada Rules on Loblaw Gift Card Program

Last week, the Privacy Commissioner of Canada determined that Loblaw Companies Ltd. initially collected more personal information than it needed with respect to the $25 Loblaw gift cards it made available to customers affected by a bread price-fixing scheme in which Loblaw participated. Specifically, Loblaw should have advised, and later did advise, prospective gift card holders that they could redact personal information that did not verify eligibility for the gift card program from the copies of utility bills or driver licences information. More interestingly, the Commissioner accepted as compliant with federal privacy law (PIPEDA) Loblaw's privacy policy and related consent Loblaw obtained from prospective gift card holders to share their personal information with the third parties Loblaw engaged to handle its gift card program, including a third party in the U.S.

Scope of Information Collected Offside

In late 2017, Loblaw publicly acknowledged its participation in a bread price-fixing scheme between 2001 and 2015 and announced that it would offer $25 gift cards to affected customers. To receive a gift card, customers needed to register online. In about 10% of cases, Loblaw asked for backup identification documentation showing the individual's name and address, such as a utility bill or driver's licence, to authenticate the individual. A complainant alleged Loblaw was collecting more personal information than was necessary to carry out the gift card program.

Loblaw maintained that the utility bill and driver's licence information was meant to ensure the gift cards were issued only to identifiable, eligible individuals and to safeguard against fraud; once the information was verified, it was immediately destroyed. Loblaw later clarified in the media, on its website and in its form of request for backup documentation, that it was only seeking to confirm that an individual resided at the address provided on the registration form and that other sensitive information (such as a driver's licence number) could be redacted from the backup documentation.

The Commissioner determined that, while the request by Loblaw for documentation confirming name and address would, in certain identified circumstances, have been necessary to ensure that only eligible individuals received a gift card and to prevent fraudulent requests for multiple cards, Loblaw was collecting, at least initially, more information than necessary to fulfil these purposes by asking for full copies of the identification, when it only needed proof of name and address. As Loblaw had already taken steps to clarify the scope of its collection of identification, the Commissioner determined that, although Loblaw's actions contravened the applicable privacy legislation, the matter had already been resolved by Loblaw.

Privacy Policy and Consent

The Commissioner also examined whether Loblaw failed to comply with the law by sending personal information about gift card holders to the Canadian and U.S. third parties it engaged to administer the program. Loblaw's applicable privacy policy identified these third parties and how customer's personal information would be used:

> 1. Scope & Interpretation
>
> … The Loblaw Card Program is administered by JND Legal Administration (the "Program Administrator") on behalf of Loblaw. Blackhawk Network (Canada) Ltd. ("Blackhawk") ***will be fulfilling and distributing the cards as well as tracking their activation and use on behalf of Loblaw***, and

Authors

Daniel Cohen
dcohen@goodmans.ca
416.597.5494

Monique McAlister
mmcalister@goodmans.ca
416.597.4255

Peter Ruby
pruby@goodmans.ca
416.597.4184

> Peoples Trust Company ("Peoples") ***will act as the card issuer on behalf of Loblaw***"…
>
> 4. How Your Personal Information Will Be Used and Shared
>
> Your Personal Information ***will be used to verify your eligibility to receive a $25 Loblaw Card, communicate with you, fulfill and distribute cards, process card transactions, verify your identity, provide customer service, process claims for lost or stolen cards, reduce the risk of fraud, track and prove card activation and use, and for any other purpose authorized or permitted by law.*** The Personal Information submitted by you ***may be shared*** amongst Loblaw, the Program Administrator, Blackhawk and Peoples for the purposes referred to above… [Emphasis added.]

Loblaw's privacy policy also expressly dealt with the role of the third party providers and the transfer of personal information outside of Canada:

> 5. Retention and Cross-border Transfer
>
> Personal Information ***may be stored, accessed, or used in a country outside of Canada by Loblaw, the Program Administrator, Blackhawk and/or Peoples, or by service providers engaged by any of them, for any of the purposes identified in Section 4 above including the United States and El Salvador.*** Where Personal Information is located outside of Canada, it is subject to ***the laws of that jurisdiction*** which may differ from those in your jurisdiction and any Personal Information transferred to another jurisdiction ***will be subject to law enforcement and national security authorities in that jurisdiction***. Subject to these laws, Loblaw, the Program Administrator, Blackhawk and Peoples will use ***reasonable measures to maintain protections of your Personal Information that are equivalent to those that apply in Canada.*** You hereby ***give your consent*** to such cross-border transfers (including to El Salvador and to the United States) of such Personal Information for any of the purposes set out in Section 4, above. [Emphasis added.]

The Commissioner also examined the contracts between Loblaw and two of its third party service providers, noting the safeguards in place:

> The contract also provided guarantees of confidentiality and security of personal information, and included a list of specific safeguard requirements, such as: (i) implementing measures to protect against compromise of its systems, networks and data files; (ii) encryption of personal information in transit and at rest; (iii) maintaining technical safeguards through patches, etc.; (iv) logging and alerts to monitor systems access; (v) limiting access to those who need it; (vi) training and supervision of employees to ensure compliance with security requirements; (vii) detailed incident response and notification requirements; (viii) Loblaw's pre-approval of any third parties to whom JND wishes to share personal information, as well as a requirement for JND to ensure contractual protections that are at a minimum equivalent to those provided for by its contract with Loblaw; and (ix) to submit to oversight, monitoring, and audit by Loblaw of the security measures in place.

Loblaw confirmed that its contract with another third party provider included similar safeguards to those required under its contracts described above. These, in turn, included a requirement for the provider to ensure contractual protections that are at a minimum equivalent to those provided for by its own contract with Loblaw when sub-contracting.

The Commissioner concluded that, "given the limited, albeit sensitive, information that was shared with the Program Administrator, as well as the limited purposes and duration for which that information would be used, Loblaw's detailed contractual requirements were sufficient to ensure a level of protection that was comparable to that which would be required under the Act", and found Loblaw was in compliance in this regard. The Commissioner was also satisfied that "the purposes for which the name and address information was transferred for processing were consistent with those for which consent was originally obtained, such that additional consent for the transfer was not required" and that the privacy policy disclosure was sufficiently transparent.

Takeaways

There are several takeaways from the Commissioner's finding:

- Even when collecting a document, individuals should be advised that they may redact the portion of the document that conveys personal information not required for the organizations's stated purpose. A privacy policy can use direct simple language to disclose how an organization intends to use personal information, transfer it to other jurisdictions, and share it with third parties.

- During a complaint investigation, the Commissioner will look at the underlying agreements with respect to the protection of personal information.
- The list of protective measures accepted by the Commissioner is a useful guide when drafting third party processing agreements. The Commissioner appeared to approve of there being "detailed contractual requirements".
- Unlike in the Equifax finding earlier this year, discussed in our April 15, 2019 Update, *Privacy Commissioner Reverses its Position on Cross-Border Transfers of Personal Information,* the transfer of personal information to a third party, even to a party located outside Canada, does not require consent: only reasonable and adequate notice is required. This is consistent with the Commissioner's 2009 *Guidelines for processing personal data across borders*, which it recently reconfirmed as discussed in our September 24, 2019 Update, *Privacy Commissioner Retains Original Policy on Cross-Border Transfers of Personal Information*.

For further information on the Commissioner's ruling, please contact any member of our Privacy, Technology or Litigation Groups.