The Three C's – Cannabis, Collection and Canada: Regulators Issue Guidance on Protecting Personal Information in Cannabis Transactions

April 1, 2019

By Amanda Branch and Jennifer McKenzie

Recreational cannabis became legal in Canada on October 17, 2018 and privacy-conscious consumers quickly voiced concerns about the collection of personal information, particularly during the purchasing process.

One of the stated purposes of the "Cannabis Act", the federal law that legalizes cannabis, is "to provide for the licit production of cannabis to reduce illicit activities in relation to cannabis". However, there have been some reports about the perception among consumers that one of the main advantages of purchasing from the illicit market is that cash transactions have no paper trail so privacy is preserved. This is especially true in those provinces where the retail sales is publicly and not privately run. (It is reported that the black market continues to thrive because of the supply issues experienced by the legal channels of trade, but that's another issue!) Even though recreational cannabis is legal in Canada, it remains illegal in most other countries, and there is arguably still a stigma surrounding the recreational use. As a result, privacy is paramount.

In December 2018, the Office of the Privacy Commissioner of Canada (the "**OPC**") released guidance titled Protecting personal information: Cannabis transactions (the "**OPC Guidance**"). The OPC Guidance is adapted from an earlier document released by the Office of the Information and Privacy Commissioner for British Columbia called Protecting personal information: Cannabis Transactions, (the "**BC Guidance**").

The *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") applies to private sector organizations in Canada that collect, use, or disclose personal information in the course of commercial activity, except where that activity takes place entirely within a province with "substantially similar" legislation (currently Quebec, Alberta and British Columbia). The British Colombia *Personal Information Protection Act* ("**PIPA**") applies to any private organization that collects, uses and discloses the personal information of individuals in British Columbia.

Personal information is any "information about an identifiable individual". This is a very broad definition and can include things like name, address, government-issued identifiers, health information and medical records, financial information and biometric data.

Data collection: Collect only what is necessary

Under PIPEDA and PIPA, businesses may collect personal information only to the extent that it is necessary for the purposes identified by the organization (see here for our discussion on the OPC's Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)). These purposes must be in line with what a reasonable person would consider appropriate in the circumstances.

Organizations must also obtain consent before collecting any personal information, subject to limited exceptions. In particular, individuals must be made aware of what personal information is being collected, to which parties it will be disclosed, the purposes for its collection, and any residual risks of harm (see here for our discussion on the OPC's Guidelines for obtaining meaningful consent).

PIPEDA recognizes that there are circumstances where consent is implied. For example, when you purchase a product online, the retailer has implied consent to collect your credit card number, the name as it appears on your credit card, and

your billing and shipping address, all for the purpose of completing the purchase transaction.

Both guidance documents advise cannabis retailers to:

- Collect the least amount of personal information possible and ensure it is stored securely;
- Refrain from recording personal information where possible (e.g., while in-person cannabis transactions require cannabis workers to request and review identification such as a driver's license, the BC Guidance expressly states there is no need to record this information in that province).
- Consider collecting email addresses only (no names) for mailing lists or memberships, however, retailers will have to ensure that their promotions by email or mail do not run contrary to the Cannabis Act. Specifically, the Cannabis Act states that "informational promotions" and "brand preference" promotions may be sent by mail to an individual over 18 years of age who is addressed by name. Obviously then, this would which require the collection of personal information beyond that of an individual's email address alone; and
- Determine whether less privacy-intrusive alternatives to video surveillance are appropriate. Recall that using video surveillance to monitor the store results in capturing an individual's image or voice (this is a collection of personal information)

Similarly, both guidance documents offer the following suggestions to consumers:

- Be aware of what personal information you are providing, particularly through online transactions which may carry additional security risks.;
- Consider using cash to purchase cannabis if the option is available, particularly if the consumer is concerned about using a credit card. Practically speaking, this option may not always be available, depending on how cannabis is sold in a province. For example, in Ontario, to date, the only ability to legally purchase cannabis is online through the Ontario Cannabis Store making credit card transactions a necessity. However, following a lottery for retail licenses, this is about to change as soon first bricks and mortar stores get up and running;); and
- Evaluate the risks involved when providing personal information to join a membership club or mailing list, and ask how your personal information will be stored.

Protecting personal information and creating policies

Both guidance documents note that cannabis retailers:

- Must designate a person who is responsible for ensuring compliance with the applicable legislation. The name, position title and contact information must be disclosed upon request.
- Must protect the personal information in their custody or under their control using security safeguards that are appropriate to the sensitivity of the information.
    - This includes physical (e.g., locked or secured information, cross-shredding documents, etc.), technological (e.g., unique IDs and passwords for each user, encryption, firewalls, etc.) and organizational security measures (e.g., mandatory staff training, restricting employees from only the personal information that is required for their role, etc.).
- Can use personal information only for the purpose for which it was originally collected and should keep personal information only for as long as necessary to fulfill that purpose.
- Should conduct periodic audits and risk assessments to ensure controls are up to date.
- Must develop internal policies and practices to meet responsibilities under PIPEDA and/or PIPA. Organizations should ensure protection of personal information is a priority and that all management and staff receiving training. The BC Guidance specifically recommends mandatory training for new employees as we all regular refresher training.
- Must create external privacy policies and notices that provide individuals with sufficient information about the organization's privacy practices.

The both guidance documents state that the personal information of cannabis users is considered very sensitive, particularly because cannabis is illegal in many countries outside Canada and, as a result, Canadian cannabis users may be denied entry to a foreign country if it is known they have purchased cannabis, even if done legally. As a result, retailers should consider storing personal information inside Canada and use caution if storing in the cloud or on a third party proprietary system, particularly if these are located outside Canada, as that could result in the personal information being accessed by foreign law enforcement.