COMPLIANCE REPORT 21-02

Review of private liquor and cannabis retailers

JUNE 22, 2021
CANLII CITE: 2021 BCIPC 31
QUICKLAW CITE: [2021] B.C.I.P.C.D. NO. 31

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

Private sector liquor and cannabis retailers are tasked with collecting our personal information. And for good reason. They need to verify age by checking a driver's license, they capture video using surveillance systems to ensure security, they use our financial information for payment, and they collect employee information for HR and payroll purposes. Retailers' authority to collect this kind of information is found in BC's *Personal Information Protection Act* (PIPA).

Personal information collected by retailers can be very sensitive, and in the case of liquor and cannabis retailers this is especially so. One reason is that cannabis is illegal in many jurisdictions outside of Canada, with the result that some countries will deny entry to individuals who have purchased cannabis or work in the industry. Liquor sales carry their own sensitivities and stigmas that could affect an individual should a breach occur.

What this report reveals is that a number of liquor and cannabis retailers have considerable work to do in order to ensure the privacy and security of the personal information they collect is kept in accordance with the law.

While we found that some retailers do have processes in place to protect the personal information of their customers and staff, many weren't aware that they collect personal information. This leads to the obvious question of how retailers can ensure they are protecting personal information if they don't recognize the fact they are collecting it. Delegating a privacy officer, drafting policies and taking an inventory of personal information holdings are just the first but important steps in complying with privacy legislation.

We also found that a small number of retailers collect biometric information from staff, customers, or both. In one case, a retailer told us they use facial recognition as part of their surveillance system. Unless there are exceptional circumstances to consider, BC cannabis and liquor stores are not authorized to use facial recognition technology. This practice should stop immediately.

Our goal with this report was to identify any gaps in the protection of customer and employee personal information and provide resources and education. Just as they secure their product inventories, we call on retailers to safeguard the privacy of their customers and employees by maintaining privacy management programs with adequate resources, privacy officers, policies, training, and risk assessment.

It is my hope that this report generates awareness across the liquor and cannabis sectors and spurs action for the benefit of those who sell, purchase, and consume liquor and cannabis products in this province.

Michael McEvoy
Information and Privacy Commissioner for BC

EXECUTIVE SUMMARY

All liquor and cannabis retailers collect personal information, though many of those we spoke with initially believed they do not. Typical examples include verifying age through checking an individual's driver's license, collecting contact information during online ordering, taking video of customers or employees via surveillance systems, and collecting employee information for HR and payroll purposes.

Privacy management programs help to set the foundation for an organization to manage the personal information they collect. In the liquor and cannabis retail sectors, serious gaps were found. This report found that liquor and cannabis retailers largely do not have adequate privacy management programs. Many retailers did not have a privacy officer, privacy policies, an inventory of personal information they collect or any training for staff or managers relating to privacy management.

While most retailers (22 of 30) failed s. 5 of PIPA because they did not have privacy policies, all retailers employed at least basic administrative, physical, and technological safeguards to protect personal information. More needs to be done to ensure safeguards are sufficient and reasonable considering the sensitivity of the personal information, and to determine whether the safeguards employed are effective at protecting personal information. Some retailers did not perform regular risk assessment or compliance monitoring activities. However, the retailers did have effective internal reporting structures in place, and are well-practiced in documenting, tracking and reporting incidents (such as suspected privacy breaches or other such incidents).

All retailers collect personal information via video surveillance and are authorized to do so under PIPA. Some of the retailers need to draft or amend their privacy policies to include video surveillance, and some need to post or improve their signage notifying anyone who enters the retail premises that video surveillance is in use and advise of the purposes for such collection of personal information.

A small number of retailers indicated that they collect biometric information from staff, customers or both. Some retailers currently have temperature scanning devices for use during the COVID pandemic, and one retailer noted that their organization uses an ID scanner. Facial recognition was not employed in either situation. One retailer noted the use of a thumbprint scanner to document employee sign in/out. Finally, one retailer reported using facial recognition as part of their surveillance system. Unless there are exceptional circumstances to consider, BC cannabis and liquor stores are not authorized to use facial recognition technology and should immediately stop such collection.

All retailers included in this review maintain a website and collect personal information online. In some instances (i.e., online ordering, membership accounts, applying for jobs) the purposes for collection may be obvious. However, websites may also collect web browser information, information submitted in a search, internet protocol (IP) addresses, and so on. Where the

purposes for collection were not obvious, retailers did not provide clear and upfront notification. In addition, very few (5 of 30) retailers had privacy policies online to detail the collection of personal information on retailer websites.

This report contains 18 recommendations for retailers to address the gaps found through the investigation. Individual reports will also be provided to retailers involved in this review. These individual reports will include recommendations specific to the retailer and provide links to guidance documents and other information to assist retailers in improving their privacy management programs, policies, and safeguards; and for retailers to consider when collecting personal information on websites or in person. In particular, retailers need to tread cautiously when considering the collection of biometric information as, in most cases, collection of this sensitive personal information will not be authorized.

1 BACKGROUND & METHODOLOGY

1.1 Background

The Office of the Information and Privacy Commissioner for BC (OIPC) conducts audits and compliance reviews to assess how effectively public bodies and private sector organizations protect personal information and comply with access provisions under the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act* (PIPA).

Under the authority of s. 36 of PIPA, the OIPC conducted a compliance review of 30 liquor and cannabis retailers. The OIPC selected liquor and cannabis retailers based on media stories and calls regarding their collection, use and disclosure of personal information, including driver's license information, facial images and (recently, due to the COVID-19 pandemic) thermal temperatures.

In addition, cannabis retailers are required to employ security cameras to cover retail and product storage areas, and all store entrances and exits.[1] Preliminary research suggests that facial recognition technology (FRT) and advanced video analytics are common in the cannabis industry, from production facilities to retail locations.[2]

[1]Liquor and Cannabis Regular Branch (LCRB). 2020. *Cannabis Retail Store Terms and Conditions: A handbook for the sale of non-medical cannabis in British Columbia.* https://www2.gov.bc.ca/assets/gov/employment-business-and-economic-development/business-management/liquor-regulation-licensing/guides-and-manuals/cannabis-retail-store-licence-handbook.pdf.

[2] See, for example: https://www.vice.com/en/article/597n73/at-cannabis-shops-face-recognition-is-already-a-thing; https://cannabexchange.com/facial-recognition-is-it-coming-to-a-cannabis-shop-near-you/; https://medium.com/universlabs/how-artificial-intelligence-and-technology-are-revolutionising-the-legal-cannabis-industry-ee12a968669c; https://www.biometricupdate.com/201901/california-startup-plans-to-add-facial-recognition-to-marijuana-dispensary-kiosks.

The personal information of cannabis users is very sensitive. Cannabis is still illegal in many jurisdictions outside of Canada, and some countries may deny entry to individuals if they know they have purchased cannabis.[3]

This review assessed retailers' privacy management programs, privacy policies, and the collection and safeguarding of personal information. In addition, the review included retailers' use of video surveillance and whether or not they employ FRT.

1.2 Methodology

1.2.1 Objectives

The key objectives of this compliance review were to:

1. Examine personal information and privacy management practices within a select number of liquor and cannabis retailers;
2. Review the extent of compliance by retailers with legislation, guidelines and their own privacy policies; and
3. Identify gaps in privacy management programs or procedures, and make recommendations to address those gaps.

1.2.2 Scope

Utilizing components of compliance assessment, operational audit, program evaluation, and process improvement, this review included:

1. Informational interviews with:
    - BC Liquor & Cannabis Regulation Branch (LCRB),
    - Alliance of Beverage Licensees (Able BC, a membership and lobbyist organization for BC private liquor and now also cannabis retailers) and
    - Association of Canadian Cannabis Retailers (ACCRES, a federal membership and lobbyist organization for cannabis retailers);
2. A review of retailers' websites for:
    - types of personal information collected online,
    - online privacy policies,
    - whether or not the retailers offer online sales and what online payment systems they use, and
    - notification or information on the purposes for collecting personal information;

[3] See OIPC guidance on Protecting personal information: Cannabis transactions.

3. Interview(s) with retailers' CEO, delegated privacy officer, or other such persons to complete a privacy management program assessment; and,
4. A review of written privacy policies and photographs of notification or signage relating to any video surveillance and other collection of personal information via video.

The scope of this review did not include:

- An audit of retailers' electronic information management systems or product sales information (other than questions about membership accounts and/or purchase histories that retailers may keep about customers); or
- Financial transactions (other than whether or not the retailer retains credit card information or other financial information).

1.2.3 Sample Selection

OIPC auditors collected a sample of 30 retailers for inclusion in the review. At the time, there were 671 liquor retailers and 234 cannabis retailers licensed by the BC Government. Auditors selected all licensed liquor retailers operating four or more retail locations and all licensed cannabis retailers with three or more retail locations in BC. This comprised of 15 liquor retailers (which included 116 to 128 liquor retail locations[4] or roughly 18% of all licensed private sector liquor retailer locations) and 15 cannabis retailers (encompassing 60 to 71 cannabis retail locations[5] or about 28% of all licensed private sector cannabis retail locations).

On a key question of whether retailers had written privacy policies, the sample provided a margin of error of roughly 6% at a 95% confidence level. Using this question as an example suggests that the sample selected for review provides an accurate representation of the population of private liquor and cannabis retailers licensed to operate at the time the sample was selected, give or take 6%, 19 times out of 20.

Though not randomly selected, OIPC auditors believe the results to be broadly reflective of a large number of BC's licensed private liquor and cannabis retail locations. Further, the findings and recommendations in this report are meant to provide information for all liquor and cannabis retailers in BC to consider and improve their own privacy management programs and practices.

[4] The number of locations listed by the Liquor and Cannabis Regulation Branch (LCRB) for the sampled licensed private liquor retailers was less than the number of locations listed online by the sampled retailers.
[5] As with liquor retail locations, the number of licensed private cannabis retail locations listed by LCRB was less than the number of locations listed by sampled retailers.

1.3 Issues for Investigation

The issues for investigation included:

1. Do liquor and cannabis retailers have a documented privacy management program, as recommended by joint guidance on privacy management programs?
2. Have retailers developed written policies and practices as required by s. 5 of PIPA?
3. Do retailers have reasonable security arrangements to protect personal information as required by s. 34 of PIPA?
4. Do retailers employ FRT in the course of their operations?
5. Are retailers' processes for collecting personal information on their websites adequate?

2 LEGISLATION & GUIDELINES

2.1 *Personal Information Protection Act* (PIPA)

The purpose of PIPA is to govern the collection, use, and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

More specifically the basic requirements of PIPA obligate organizations to:

- designate an individual(s) to be responsible for ensuring compliance with PIPA;
- have policies and practices that show how the organization complies with PIPA;
- have a complaints process, should someone wish to complain about the organization's management of personal information;
- collect, use or disclose personal information only with the consent of the individual or where PIPA permits these activities to occur without consent;
- inform individuals about the purpose for collecting personal information on or before collecting the information directly from them; and
- collect, use, or disclose personal information, with or without consent, only for purposes that a reasonable person would consider appropriate.

Organizations can also collect employee personal information without consent where the collection is reasonable for establishing, managing, or terminating the employment relationship. In this case, the organization must notify the employee that they will be collecting, using, or disclosing the employee personal information (and the purposes for doing so) before collecting, using, or disclosing the personal information.

Further, PIPA requires an organization to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks. Where an organization is using an individual's personal information to make a decision directly affecting them, they must retain that information for at least one year. When the personal information is no longer needed for legal or business purposes the organization must securely destroy it.

2.2 OIPC Guidance

2.2.1 Privacy Management Programs

The Commissioners' joint guidance on privacy management programs[6] and the OIPC's PrivacyRight webinar[7] on the same subject point to at least 10 steps for implementing an organization's privacy management program. These include:

1. **Buy-in from the top**: senior management commitment to supporting privacy, including the provision of staff and resources.
2. **Privacy officer**: having someone specifically responsible for privacy-related duties such as drafting policies, providing training, and advocating for privacy across the organization.
3. **Reporting structures**: appropriate internal reporting structures so the privacy officer and senior management know how the privacy management program is functioning.
4. **Personal information inventory**: an inventory of the types and sensitivity of personal information the organization collects, who it is collected from, how it is collected, why or how it is used and disclosed, and where the personal information is stored.
5. **Privacy policies**: an explanation of an organization's responsibilities for handling the personal information, how the information is protected, and how individuals can request access or make a complaint about the handling of their personal information.
6. **Mandatory privacy training**: ensuring that staff and volunteers who handle personal information are trained on the organization's responsibilities and expectations for privacy management.
7. **Breach response processes**: protocols for reporting suspected breaches and steps for responding to a breach (containment, evaluation, notification, prevention).
8. **Service provider management**: ensuring service providers or contractors are aware of the organization's expectations for handling personal information.

[6] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada and Office of the Information & Privacy Commissioner for British Columbia. 2012. Getting Accountability Right with a Privacy Management Program. https://www.oipc.bc.ca/guidance-documents/1435.
[7] OIPC. 2019. Webinar 1 – 10 basic obligations under PIPA. https://www.oipc.bc.ca/privacyright/webinars/.

9. **Risk assessment**: internal evaluation of whether an organization has sufficient safeguards in place to protect personal information.
10. **Review and revise**: regular review of the privacy management program, and making updates or revisions as necessary.

For more information, please refer to OIPC guidance document Getting Accountability Right with a Privacy Management Program and the OIPC's PrivacyRight webinar on Privacy Management Programs.

2.2.2 Policies & Practices

Section 5 of PIPA states that an organization must develop and follow policies and practices necessary for the organization to meet its obligations under the Act. As per the OIPC's guidance on Developing a Privacy Policy under PIPA, privacy policies should reflect the requirements of PIPA, including:

1. **Accountability**: provide a statement that the organization is accountable for compliance under PIPA, explain what PIPA is, provide the definition of "personal information" and express a commitment to privacy.
2. **Identifying purposes and limiting collection**: explain the purposes for collection of personal information, and limit collection to what is needed to meet those purposes.
3. **Consent:** explain when and how the organization will obtain consent, the type of consent (implied or express, depending on the sensitivity of the personal information), and the right to withdraw consent.
4. **Limiting use and disclosure**: identify how the organization uses and discloses personal information and limit use and disclosure to only the purposes for which is was collected.
5. **Retention**: commit to retaining personal information used to make a decision that directly affects individuals for at least one year after making that decision and once retention is no longer necessary for legal or business purposes.
6. **Accuracy**: identify measures to ensure personal information is accurate, and how individuals can correct errors or omissions in their personal information.
7. **Safeguards**: set out administrative, physical, and technological safeguards and the process for responding to suspected privacy breaches.
8. **Individual access**: identify how individuals can access their information.
9. **Challenging compliance**: identify how an individual can make a complaint and to whom.
10. **Openness**: identify where to find the privacy policy, provide contact information for the privacy officer, and note that individuals can contact the OIPC.

Please see the OIPC guidance document Developing a Privacy Policy under PIPA and the OIPC's PrivacyRight webinar on How to write a privacy policy.

2.2.3 Security Safeguards

Under s. 34 of PIPA, organizations must use reasonable safeguards to protect personal information in their custody or under their control from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks. Organizations should employ administrative, physical, and technological safeguards to protect personal information.

1. **Administrative safeguards** are organizational policies, procedures, and regular assessment and maintenance of security measures. Administrative safeguards can include employee training, confidentiality agreements, access on a-need-to-know basis, role-based access, and audits and risk assessments.
2. **Physical safeguards** are physical measures to protect personal information (including electronic information systems, buildings, and equipment) from natural and environmental vulnerabilities and unauthorized intrusion. Physical safeguards can include locking files up, restricting access to areas where files are stored, a clean desk policy, positioning screens away from public view, and adequate disposal processes for paper files and electronic equipment containing personal information.
3. **Technological safeguards** are the technological policies and procedures that protect personal information and access to it. Technological safeguards can include using strong and secure passwords, auto log out, firewalls, intrusion detection and antivirus software, and adequate encryption.

Please see OIPC's guidance document A Guide to B.C.'s Personal Information Protection Act, PrivacyRight webinars on Security safeguards, and Securing personal information: A self-assessment for public bodies and organizations.

2.2.4 Video Surveillance

Personal information collected via video surveillance must be authorized by consent or an authority that allows for collection without consent, such as when the collection is required or authorized by law.

In either case, the collection must be reasonable and appropriate in the circumstances. For video surveillance, factors to consider when deciding if the collection is reasonable can include whether there is a specific need that surveillance is likely to be effective in meeting, the loss of privacy is proportional to the benefit gained, and other less-intrusive methods (i.e., intrusion detection, theft protection) are unlikely to meet the intended purposes.[8]

In BC, both the *Liquor Control and Licensing Act* s. 31(2)(h) and the *Cannabis Control and Licensing Act* s. 32(1)(g) authorize the general manager[9] to impose terms and conditions related

[8] K. E. Gostlin Enterprises Ltd., Re, 2005 CanLII 18156 (BC IPC), https://canlii.ca/t/1kw1r, paras 51 to 60.
[9] The general manager is a government employee, appointed by the BC Attorney General to administer the *Liquor Control and Licensing Act* and the *Cannabis Control and Licensing Act* and regulations respective to each Act. The

to the safety of employees, patrons and the public. For cannabis retailers, video surveillance security measures are detailed in the Cannabis Retail Store Terms and Conditions handbook.

These include:

6. Security cameras with full unobstructed view of:
    a. the retail sales area
    b. any product storage area
    c. both the interior and exterior of all store entrances/exists.[10]

Due to the terms and conditions made under the Cannabis Control and Licensing Act and listed in the handbook, licensed cannabis retailers are authorized by s. 12(1)(h) of PIPA to collect such personal information without consent.

In contrast, the Liquor Retail Store Terms and Conditions do not include a requirement for video surveillance so liquor retailers cannot rely on the same provision of PIPA. Instead, liquor retailers rely on consent for the collection of personal information via video surveillance. This consent can be *implicit*, such as when notice is provided and the individual decides to provide their personal information by entering the area under surveillance.

Regardless of whether the collection of personal information by video surveillance is through consent or authorized by law, organizations must provide notification. Section 10 of PIPA mandates that organizations provide notification on or before collecting the personal information. Such notice must include the purposes for collection. In addition, *upon request*, organizations must provide the position name or title and contact information for an employee who can answer questions about the collection.

Retailers should position cameras to capture the least amount of information needed to address the areas for video surveillance, and should be aware that PIPA's requirements to develop appropriate policies, practices and safeguards also apply to personal information collected by video surveillance.

Policy relating to the collection of images via video surveillance may comprise part of the organization's overall privacy policy or a stand-alone document. The policy should explain (and not be limited to):

- the rationale and purpose for surveillance;
- when and how monitoring and/or recording will be in effect;
- how recordings will be used;
- who may access recorded images;

---

general manager is responsible for, among other things, issuing licenses, supervising licensees and the operation of establishments, and enforcing the Acts and regulations.

[10] Liquor and Cannabis Regular Branch (LCRB). 2020. *Cannabis Retail Store Terms and Conditions: A handbook for the sale of non-medical cannabis in British Columbia*. Page 12.

- how long records will be kept;
- how they will be securely destroyed; and
- how to manage unauthorized access or disclosure.

See the joint Commissioner guidance on Overt Video Surveillance in the Private Sector and the OIPC's PrivacyRight webinar on Understanding consent and notification for further information.

2.2.5 Collection of Biometric Information

Biometrics is the technology of measuring, analyzing, and processing the digital representations of unique biological data and behavioral traits such as fingerprints, retinas, irises, voice and facial patterns, gaits and hand geometry. Such biometric information is particularly sensitive personal information.

If retailers are considering any type of biometric collection, authorization to utilize such technologies must be scrutinized at a very high level. The purposes for collection, use or disclosure of biometric information must be reasonable and *express consent*[11] from individuals is generally required.[12]

The OIPC has received calls to the office and reviewed media stories concerning liquor and cannabis retailers' use of ID scanners, thermal temperature devices, and FRT. With regard to ID scanners, while the Patronscan system facilitates age verification, it is not collecting or creating biometric templates from individuals' photo IDs nor from images of the individuals themselves. As for the potential that FRT may be employed within retailers' thermal temperature scanners or video surveillance systems, even with consent, it would not be reasonable to collect sensitive biometric information from every individual entering or walking by the store.

As such, unless there are exceptional circumstances to consider, BC cannabis and liquor stores are not authorized to collect biometric information. Such a collection is not what a reasonable person would consider appropriate in the circumstances, as the sensitivity and invasiveness exceed what is needed to fulfil the purpose(s) for collection.

For more information specifically on the use of facial recognition, please see the Office of the Privacy Commissioner of Canada's guidance Data at Your Fingertips: Biometrics and the Challenges to Privacy and Automated Facial Recognition in the Public and Private Sectors.

2.2.6 Collection of Personal Information on Retailer Websites & Website Privacy Policies

All retailers included in the sample for review maintain webpages for their business, and it is likely that all collect some form of personal information online. Some of this collection will be

[11] Express consent is when individuals agree (verbally or in writing) to the collection, use or disclosure of their personal information for a particular purpose.
[12] See Joint investigation of Clearview AI, 2021 CanLII 9227 (PCC), paras 38. https://canlii.ca/t/jd55x.

overt and directly from the individual, such as completing forms for membership, ordering online, signing up for newsletters or contacting the retailer. Some collection of personal information may be more covert or less obvious, such as typical website collection of device identifiers such as internet protocol (IP) addresses, browsing history, and location information, particularly if these can be linked back to an individual.

PIPA requires organizations to notify individuals of the purpose of collection unless the purpose is obvious and the individual voluntarily provides their personal information for that purpose. While the purposes for the collection of personal information directly from customers, such as to make a purchase or to sign up for a newsletter, may be obvious and consent implied; the purposes for the collection of browser information or other online identifiers may not be obvious. In the case that these less obvious identifiers can be attributed to an identifiable individual, then notice is required for their collection.

Web-based privacy policies are also an important part of ensuring the organization meets its obligations under PIPA in respect of personal information collected online. These policies are generally not a substitute for notice, as they are often too far removed from the point of collection, and include details and descriptions that obscure the simple and direct requirement for notice.

While web-based privacy policies can be part of an organization's overall privacy policies, it is important to ensure that the types of personal information collected from the website are contemplated and documented in the policy.

See OIPC's *Practical Suggestions for your Organization's Website's Privacy Policy* for more information.

3 FINDINGS

While the findings in this report reflect the state of privacy management programs within 30 of the BC private sector liquor and cannabis retailers, the results do raise issues related to privacy management policies and practices that will be of relevance and interest to all such retailers across the province.

3.1 Personal Information Collected

All liquor and cannabis retailers collect personal information, though many initially believed they do not. PIPA defines personal information as "information about an identifiable individual", including employee personal information. This is a broad definition that can include, for example: name, date of birth, driver's license number, medical information, physical description, image, social insurance number, and financial information (such as a credit card number). PIPA applies to personal information whether the information is recorded or not.

An example of a collection under PIPA is viewing a driver's license for the purpose of determining whether a customer is of legal age to purchase liquor or cannabis.[13]
Typical customer personal information collected by liquor and cannabis retailers included:

- age verification through driver's license or BC ID;
- contact information for online ordering (name, phone number, email address);
- payment information;
- member information (contact information and, in some cases, purchase history);
- delivery transaction records (date, time and address of delivery, products purchased, prices charged, quantity, delivery fees, and name and signature of recipient);
- newsletter sign-up (name, email address);
- web and computer information (IP address, geographical location of IP address, login credentials); and
- photographs or video surveillance images.

Typical employee personal information collected included:

- contact information (including emergency contact information);
- hiring information (resumes, credentials);
- security clearance and worker verification (background checks);
- payroll and tax information (social insurance number, birthdate, bank information);
- benefits and beneficiaries (claims information, partner and dependents names);
- learning and employee performance (certificates earned, learning plans, performance reviews);
- photographs or video surveillance (some retailers collect employee consent forms); and
- other personal information, such as
    - food allergies or
    - COVID-19 health information (questionnaire on symptoms, travel, etc.).

Please see the OIPC's Guide to PIPA for more information on identifying personal information under an organization's control and the OIPC's PrivacyRight webinar on the Authority to collect, use, and disclose personal information.

[13] OIPC Order P10-01. [2010] B.C.I.P.C.D. No. 7. https://www.oipc.bc.ca/orders/1418.

3.2 Privacy Management Programs

Privacy management programs help to foster respect for privacy and help organizations to meet their legislative obligations under PIPA. To assess retailers' privacy management programs, OIPC auditors reviewed retailer websites and privacy policies, and interviewed key personnel. Job titles for key personnel who took part in the interviews included Chief Executive, Operations or Financial Officer; President; General Manager; Regional Manager; Director of Operations; Senior Legal Counsel or Director of Human Resources.

These personnel were generally knowledgeable within their field. Years of experience in their respective retail industry varied from 1.5 to 13 years in the cannabis retail sector (average of four years of experience) and 1.5 to 33 years in the liquor retail sector (average of 13 years of experience). In the cannabis sector, interviewees included the time or experience they gained prior to legalization in 2018.

As noted earlier, this review included all licensed private sector retailers with at least three (cannabis) or four (liquor) storefronts in BC. Cannabis retailers employed anywhere from 15 to 100 staff (with an average of 46 staff) and liquor retailers employed 30 to 143 staff (with an average of 88 staff). These numbers did not include bookkeepers, information technology contractors, shredding companies, or other contractors who may have access to the personal information retailers collect from customers or staff. This means that privacy management programs should be robust enough to account for the various individuals and transactions inherent to the processing of personal information from collection to destruction.

The current size of operation within the licensed private sector cannabis retailers, being a relatively new type of organization, is smaller than that of liquor retailers. The same can be said for the years of related work experience. However, several private cannabis retailers reported they will be expanding the number of locations and staff in the near future. Regardless of size, all retailers, like other organizations, are equally responsible for ensuring appropriate management of the personal information they collect, use and disclose. Adequate privacy management programs will ensure compliance with the respective legislative requirements.

As shown in Table 1, the policy review and interviews revealed that the sampled liquor and cannabis retailers largely do not have adequate privacy management programs. Without a fulsome privacy management program, organizations may not have sufficient policies and practices to effectively meet their legislated obligations under PIPA. Discussion of each aspect follows.

TABLE 1 THE NUMBER OF RETAILERS WITH ELEMENTS OF A PRIVACY MANAGEMENT PROGRAM

	Liquor Retailers	Cannabis Retailers
1. Buy-in from the top	6	6
2. Privacy officer	6	5
3. Reporting structures	15	15
4. Personal information inventory	1	1
5. Privacy policies	6	4
6. Mandatory privacy training	0	0
7. Breach response processes	13	10
8. Service provider management	6	8
9. Risk assessment	9	8
10. Review and revise	7	3

3.2.1 Buy-in from the top

Support from the executive is critical for any organization's privacy management program to be adequate and effective. The head of the organization, such as the CEO or owner, is ultimately accountable for ensuring the organization meets its legislated obligations. This includes providing adequate resources and staff for privacy management and promoting privacy management across the organization.

When asked whether the organization has the resources and buy-in from the top, less than half of all 30 retailers (6 liquor, 6 cannabis) agreed.

RECOMMENDATION 1

Retailers should ensure adequate funding and resources for effective privacy management programs.

3.2.2 Individual responsible for PIPA

PIPA s. 4(3) mandates that organizations designate one or more individuals to be responsible for ensuring the organization complies with the Act. Very few retailers had designated someone as a privacy officer for their organization: only six of 15 liquor retailers and five of 15 cannabis retailers had someone specifically responsible for privacy management.

The remaining retailers have failed to comply with this requirement of PIPA. In some cases, interviewees were able to identify the person who would likely perform the role but the individual had not been designated by the CEO or owner as having specific responsibility for privacy functions.

RECOMMENDATION 2

Retailers without privacy officers should immediately designate one or more individuals to be responsible for ensuring the organization complies with PIPA.

Interviewees from retailers with designated privacy officers noted that the basic job duties for the privacy officer include:

- establishing and updating the privacy policy and employee handbook;
- training staff and managers and ensuring privacy and confidentiality are maintained;
- ensuring adequate signage for surveillance, and ensuring that information is handled and stored correctly;
- decision-making when it comes to infrastructure, data storage, servers and/or working with the IT team to make sure data is safe and secure;
- conducting risk assessments and compliance review of policies and programs, and reporting compliance to meet provincial regulations;
- responding to privacy complaints or requests, for example if a customer has asked for their data to be removed from the system(s); and
- managing suspected breaches.

Resources are available at www.oipc.bc.ca, including guidance documents and webinars to educate privacy officers and others about PIPA and privacy management duties and functions.

3.2.3 Internal reporting structures

Internal reporting structures are the processes that "ensure that the right people know how the privacy management program is structured and whether it is functioning as expected."[14] This includes clearly documenting and communicating reporting and escalation procedures so staff at all levels know how and with whom to raise privacy issues, conducting compliance

[14] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada & Office of the Information & Privacy Commissioner for British Columbia. 2012. Getting Accountability Right with a Privacy Management Program. P.8. https://www.oipc.bc.ca/guidance-documents/1435.

monitoring and risk assessments, and ensuring that the CEO or owner is aware of how privacy management is functioning within the organization.

All 30 of the cannabis and liquor retailers noted that staff know to whom and how to report privacy-related concerns and that internal reporting structures, even if not documented, are clear within and across the organization. Several interviewees mentioned that all staff are aware of the licensing requirement to maintain incident logs of any issue that occurred during the day and, while not privacy-specific, privacy incidents would be documented in the same location as well. Logs are often kept in an online reporting system, or in binders that management reviews daily.

Logged incidents may include:

- occasions where staff have denied someone service if they were identified as a minor or were acting in a belligerent manner;
- any harm or physical accidents involving staff or customers;
- any theft, robbery or attempted robbery; or
- other issues.

Interviewees noted that their staff know to raise serious issues right away with the store manager. In addition, interviewees stated that staff can raise issues of different kinds with the manager, HR or anyone above those roles.

3.2.4 Personal information inventory

As noted above, liquor and cannabis retailers may collect a large amount of personal information from customers, members, employees, and others who enter their stores. For customers, this ranges from checking a customer's ID to collecting contact information, purchase histories, web and computer information, and payment information. For employees, this typically includes contact and hiring information, security clearance and work verifications, payroll and tax information, benefits and beneficiary information and learning and performance history. Video surveillance captures images of every individual who enters the stores.

Only two of 30 retailers (one liquor, one cannabis) indicated that they maintain a personal information inventory. While many retailers noted that their Point-of-Sale (POS) system stores the personal information, this is not a personal information inventory. A personal information inventory is a specific list or document that details:

- the types of personal information collected and the type of individual (i.e., employee or customer) the information is about; and for each type of personal information:
- the purpose for collecting, using or disclosing each type of personal information;
- the sensitivity of the personal information collected; and

- where the personal information is held.

A personal information inventory helps organizations keep track of the personal information they collect, to be able to quickly identify relevant information if someone requests their own personal information or to determine what information may have been affected in the event of a breach. The inventory can also help to establish retention needs and to determine if the organization still needs to collect each type of information.

RECOMMENDATION 3

Retailers should develop and maintain an inventory of all types of personal information they collect, the purposes for collection, where the information is stored, and its sensitivity.

3.2.5 Written privacy policies

All organizations under PIPA are required to have policies and practices necessary to meet their legal obligations. PIPA s. 5 states:

> 5 An organization must
> (a) develop and follow policies and practices that are necessary for the organization to meet the obligations of the organization under this Act,
> (b) develop a process to respond to complaints that may arise respecting the application of this Act, and
> (c) make information available on request about
> (i) the policies and practices referred to in paragraph (a), and
> (ii) the complaint process referred to in paragraph (b).

In addition to being required by PIPA, fulsome privacy policies are an essential component of a privacy management program. They set the expectations for all staff on the appropriate collection, use and disclosure of personal information. Privacy policies, and the communication thereof, are a fundamental part of meeting an organization's legal duties.

OIPC auditors requested the retailers to provide written privacy policies for review. Of the 30 retailers, 16 retailers provided privacy policies or other materials in response:

- 10 provided privacy policies;
- three provided a sheet on safeguards;
- two provided documents pertaining to employee personal information only;
- one provided a protocol for responding to privacy breaches.

Only the privacy policies were included in the analysis. Two of the privacy policies, along with the remaining documents listed above, did not contain sufficient aspects of a privacy policy. With this, eight retailers had privacy policies that reasonably contained the essential aspects of privacy policy.

This means that 22 of 30 retailers failed to meet their obligations under s. 5 of PIPA. The aspects to include in a privacy policy are discussed in the next chapter of this report.

RECOMMENDATION 4

Retailers must develop and maintain policies and practices necessary to meet the obligations under PIPA.

3.2.6 Mandatory privacy training

None of the 30 retailers, which comprise approximately 1,200 employees, provide mandatory privacy training for their staff. Twelve retailers (8 cannabis, 4 liquor) noted that during the orientation of new hires, staff are asked to sign a confidentiality agreement. One additional cannabis retailer reported that management also sign such agreements.

The importance of mandatory privacy training and refresher privacy training cannot be over-stated. Without this, retailers are failing to meet their obligation to provide reasonable security arrangements under s. 34 of PIPA.

RECOMMENDATION 5

Retailers should provide mandatory privacy training and education for all staff, managers, contractors and others who may access the personal information the organization collects.

RECOMMENDATION 6

Retailers should ensure that all staff, managers, contractors and others who may access the personal information review the clinic's privacy policies and sign a confidentiality agreement.

3.2.7 Breach response processes

Written breach response processes set the expectations for how staff and contractors should respond when there is unauthorized access to or collection, use, disclosure or disposal of personal information. The basic steps should include:

- containment of the breach;
- evaluation of the risk of harm to affected individuals;
- notification of affected individuals, where relevant; and
- actions to prevent future breaches.

Inline with discussion on retailers' internal reporting structures, several retailers (13 liquor, 10 cannabis) have established processes that staff are to follow in the event of a suspected breach. As discussed above, suspected breach incidents would typically be reported directly to store managers or summarized in the daily logs for management to review.

Privacy policies for one cannabis retailer included provisions for managing breaches, and one liquor retailer had a policy specific to privacy breach response protocols. Otherwise, the remaining 28 retailers did not have documented breach response processes. Contemplation and documentation of breach response, including containment, evaluation of risk, notification, and prevention is essential for protecting personal information under s.34 of PIPA. Staff should also be made aware of this process and, in particular, who to contact in the event of a suspected breach.

RECOMMENDATION 7

Retailers should establish, document, and communicate clear breach reporting and response processes.

For more information on managing breaches please see the OIPC guidance document Privacy Breaches: Tools and Resources and the OIPC's PrivacyRight webinar on Security Safeguards.

3.2.8 Service provider management

Sections 17 through 22 of PIPA cover the circumstances for which organizations may disclose the personal information they collect from staff, customers, or others. Generally, retailers may disclose personal information to service providers or contractors for the purposes for which they collected the information and to assist the service provider or contractor to carry out work on the retailers' behalf. Most of the retailers (22 of 30) indicated that they used contractors and services providers, though roughly half (6 liquor retailers, 8 cannabis) reported having contracts or non-disclosure agreements in place that include detail about the retailers' expectations with regard to privacy and security.

Interviewees provided examples of contractors or service providers their retailer uses, including for:

- IT security;
- POS systems;
- Payment processing (rely on third-party's service agreement); and
- External bookkeeping or accounting for payroll and accounting purposes.

Of the 14 retailers who noted they have documented expectations, some noted that they rely on service agreements provided by the third-party organizations, which include confidentiality provisions, for contracts with POS systems or payment processors. One retailer also reported that their organization has contractor orientation and training, which includes reviewing privacy guidelines.

Other retailers who rely on service providers or contractors told OIPC auditors that they have a general contract in place but it does not detail expectations related to managing personal information, or that they have an informal, verbal or established trust with long-standing service providers but nothing in writing to detail privacy and security expectations.

Liquor and cannabis retailers, like any other organization, cannot contract out of their legislated obligations under PIPA. The retailer is responsible should a service provider or contractor breach any aspect of the legislation.

RECOMMENDATION 8
Retailers should ensure written contracts and information sharing agreements are in place and express expectations for privacy protection.

The OIPC's guidance on Information Sharing Agreements and the OIPC's PrivacyRight webinar on Using and Disclosing Personal Information may be of assistance.

3.2.9 Risk assessments

Just over half of the retailers (17 of 30; 9 liquor and 8 cannabis) reported that they conduct risk assessments, internal audits, IT Security, physical security, privacy impact assessments or other compliance monitoring activities. When asked how they know whether the personal information they collect is kept secure, the other retailers noted that it is impossible to know for sure whether information is secure, that they trust their own or service providers' systems, or that they did not believe they collected any personal information.

Without regular risk assessment and compliance monitoring processes in place, retailers fail to meet obligations under s. 34 of PIPA to make reasonable security arrangements to safeguard the personal information in their custody or under their control.

RECOMMENDATION 9

Retailers should conduct regular risk assessment and compliance monitoring activities and mitigate risks to personal information privacy and security.

The OIPC's PrivacyRight webinar on Risk Management and Compliance Monitoring may be of assistance.

3.2.10 Review and revise

Regular review of a privacy management program is necessary to ensure that policies and practices for handling and securing personal information are effective. Organizations should reflect on their overall program to determine if they need to make any changes.

For example, the COVID-19 pandemic thrust many retailers into online ordering and sales platforms. Therefore, retailers need to ensure that policies and safeguards keep pace with information security, staff are aware of the sensitivity of personal information in the context of liquor and cannabis retail, and access is limited to only those who need that personal information for their work. Similarly, with video surveillance, retailers need to consider and limit who can access images, and ensure processes for saving extracts or disclosing such information to the police are well-documented and each occasion logged for review.

Essentially, retailers must ensure that their privacy management program is well-documented, communicated to staff, tested to determine its efficacy and reviewed regularly to ensure it is kept current.

Ten of the 30 retailers (7 liquor, 3 cannabis) reported having reviewed their privacy management program within the previous two years. An additional eight retailers, all cannabis,

noted that they reviewed their programs upon being contacted by the OIPC to take part in this review.

RECOMMENDATION 10

Retailers should develop and document an annual review plan that details how they will monitor and assess the effectiveness of their overall privacy management program.

To conclude the questions on privacy management programs, interviewees from each retailer rated their own organizations' program on a scale from one to 10, with 10 being the most fulsome. Liquor retailer self-ratings ranged from five to 10, with an average of eight. Cannabis retailers rated themselves anywhere from one to 10, with an average score of 6.

In explaining their self-assessment, some retailers noted that their organization takes privacy very seriously and is always reviewing and looking at ways to improve privacy and security. Other retailers pointed to somewhat incorrect assumptions that:

- they do not collect personal information so their privacy management program is excellent;
- the privacy management function is implicit in their day-to-day operations and does not need to be documented or formalized; and
- reliance on third-party security in their POS system minimizes the need for privacy management by the retailer.

Some retailers pointed to challenges their organization has when it comes to privacy management. These challenges included, for example:

- lack of knowledge or awareness of the requirements;
- ensuring all staff, front-line staff in particular, are trained (hard with staff turnover);
- resources in small companies means privacy officers are responsible for several other functions and are not dedicated specifically to privacy; and
- more orders and sales occurring online has increased concerns around network or system hacking and has increased reliance on third party technology consultants.

The joint guidance document Getting Accountability Right with a Privacy Management Program and the OIPC's PrivacyRight webinars on Privacy Management Programs are available to assist retailers in learning about their obligations for privacy management.

3.3 Privacy Policies

As noted in the section on privacy management programs, policies are an important foundational component and are required under PIPA. Policies should be in writing and provided to all staff, managers, contractors or others who may access personal information that the retailer collects about customers, members, employees or others. In addition, if requested, organizations must make information available about their privacy policies and their practices and processes for responding to complaints about the organization's handling of personal information. Best practice is to post privacy policies online and to make a copy available at retail locations.

Ten of the 30 retailers in this compliance review provided the OIPC copies of privacy policies. Of these, eight policies contained the majority of elements necessary to show how the organization is to meet its obligations under the Act. Please see Table 2 below for a breakdown of the necessary elements of a privacy policy, as outlined in OIPC guidance, with the number of liquor or cannabis retailers who included them in their written policy.

TABLE 2 THE NUMBER OF RETAILERS WITH ELEMENTS OF A WRITTEN PRIVACY POLICY

	Liquor Retailers	Cannabis Retailers
Written Privacy Policies	6 of 15	4 of 15
1. Accountability		
- Compliance with PIPA BC	3	2
- Define PI consistent with PIPA	4	2
2. Purpose & Limits to Collection		
- Purpose for collection	5	4
- Limits to collection	5	4
- Description of PI collected	5	2
3. Consent		
- Consent Required for Collection	5	3
- How Consent will be Obtained	5	2
- Right to Withdraw Consent	5	2
4. Disclosure of PI	5	3
5. Retention & Disposal	5	4
6. Accuracy & Correcting PI	6	3
7. Safeguards		
- Administrative	1	2
- Physical	3	2
- Technological	2	3
- Breach Response Process	0	1
8. Request Access to Own PI	6	3

9. Right to and How to Complain	5	3
10. Openness		
- Contact info for Privacy Officer	4	1
- Contact BC OIPC	3	3

The findings in Table 2 suggest that the few privacy policies submitted for review by liquor and cannabis retailers frequently missed the following:

- A statement indicating that they will comply with PIPA BC;
- Definition of personal information (to be consistent with PIPA);
- Breach response protocols; and
- Contact information for the organization's privacy officer.

Most retailers (22 of 30) failed to meet the requirements of s. 5 of PIPA. Recommendation 4 states that "retailers must develop and maintain policies and practices necessary to meet the obligations under PIPA." Best practice is for each retailer is to include the components listed in Table 2 and further defined in OIPC guidance on Developing a Privacy Policy under PIPA.

Retention Period

When reviewing the policies and during interviews with retailers, it became apparent that there is no standard practice for how long to maintain different aspects of personal information. PIPA requires that organizations retain information used to make a decision that affects an individual for one year and, otherwise, to destroy documents containing personal information once that information is no longer needed. Specifically, s. 35 states:

> 35 (1) Despite subsection (2), if an organization uses an individual's personal information to make a decision that directly affects the individual, the organization must retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.
> (2) An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that
> (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information, and
> (b) retention is no longer necessary for legal or business purposes.

Most retailers (19 of 30) noted that they retain personal information such as member purchase history *indefinitely* unless an individual requests to opt out of such retention. Two retailers noted they keep records that contain this personal information for six-to-seven years for tax purposes. One retailer noted that they keep member or purchase history for only one year.

RECOMMENDATION 11

Retailers should formulate and implement a schedule for retention of personal information that complies with s. 35, and securely destroy or remove the means by which the personal information can be associated with particular individuals in accordance with the retention schedule.

3.4 Security Safeguards

Retailers are legally responsible for all personal information under their control, even if it isn't in their custody.[15] Retailers must have procedures in place to safeguard personal information. Section 34 of PIPA states:

> 34 An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

Based on information collected through interviews and written policies, all of the retailers employed at least basic administrative, physical, and technological safeguards to protect personal information in their custody.[16]

All of the liquor and cannabis retailers reported that they have a security officer or someone in charge of physical or IT security. In many cases, retailers contracted security monitoring companies but day-to-day responsibility for physical security fell to store managers, and some stores hired security guards. For IT security, most retailers hired IT contractors for maintenance of technological safeguards, and in some cases the retailer retained the IT staff in-house. For administrative safeguards, responsibility for privacy policies, employee training, confidentiality agreements and the like, if they exist, generally fall to the privacy officer, compliance officer, HR Manager or CFO.

While relatively few (8 of 30) retailers had fulsome written privacy policies, some policies lacked sufficient detail on the kinds security safeguards retailers implemented. Three cannabis retailers who did not have written privacy policies, provided detailed documents specifically about their administrative, physical and technological security safeguards. Detail from these

[15] For example, employee personal information provided to an accounting firm that performs payroll services to the retailer is still under the control of the retailer even though not specifically in its custody.
[16] Information reported by retailers in this section has not been verified, as the OIPC did not directly inspect retailers' physical or technological safeguards.

documents along with detail from privacy policies that included a description of safeguards are included in below.

3.4.1 Administrative safeguards

Administrative safeguards described in policies or during interviews included:

- employee confidentiality agreements relating to handling personal information;
- employing "need to know" as a rule for who can access personal information and role-based access to systems;
- training all managers and supervisors how to maintain safeguards, and ensure staff receive adequate training and orientation;
- conducting privacy spot checks and reminding employees about protocols;
- conducting quarterly inspections to monitor compliance with policies and procedures; and
- conducting annual reviews of systems and processes.

The lack of written privacy policies, privacy training, and documented personal information inventories leaves an obvious gap in administrative safeguards for the majority of retailers.

3.4.2 Physical Safeguards

Physical safeguards detailed in privacy policies or during interviews included:

- locked doors, customers buzz to gain entry;
- door access monitored and recorded;
- security staff or management monitoring for incidents;
- security cameras in place to deter unauthorized activities;
- locking file cabinets and areas/offices where files are stored;
- empty desk policies whereby all documents containing personal information are stored securely when not in use;
- all documents containing personal information shredded prior to disposal;
- documents required by law or for business continuity are stored in a secure, offsite location;
- positioning computer monitors away from unauthorized personnel or customers;
- servers stored in a secure room and locked in cabinet;
- destruction of computer hard drives that contain personal information before you discard them.

During interviews, one retailer noted that employee files are stored in an unlocked filing cabinet in the senior representative's home. Even if this individual lives alone, this is not a secure method of storage.

3.4.3 Technological Safeguards

Several retailers use POS systems to manage customer information and reported reliance on third party contractors to ensure POS security is maintained. Some retailers maintained their own in-house systems and employed IT staff or hired contractors. Technological safeguards described by retailers, whether in written policies or during interview included:

- having UserIDs for staff logins and password-protected computer screensavers;
- using strong and secure passwords and changing those passwords regularly;
- modifying equipment and software so credit card or debit numbers are removed or truncated from receipts;
- using firewalls, intrusion detection software, and antivirus software;
- secure platforms and Standard Operating Procedures to mitigate unauthorized access;
- third party protected cloud databases, encryptions, 2-factor authentication;
- intrusion detection and prevention systems;
- workstation monitoring for anomalies and identified risks (e.g. a malicious email attachments);
- secure wiping of hard drives before discarding, selling or donating;
- periodic review and internal audits of security practices; and
- external system reviews by qualified security assessors.

For retailers who rely on POS systems and third-party contractors, it is not sufficient to assume that the system or contractors are maintaining adequate technological security for the personal information collected at retail establishments. Retailers should review contracts and safeguards to ensure contractors and service providers are meeting industry standards for technological security.

Retailers that do not implement relevant administrative, physical and technological safeguards and do not monitor the effectiveness of safeguards fail to meet their legal obligations to make reasonable security arrangements to prevent authorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.

RECOMMENDATION 12

Retailers should review administrative, physical, and technological safeguards and ensure they are reasonable and effective, considering the type and sensitivity of personal information their organization collects.

Please see the OIPC's Guide to PIPA , the joint self assessment on Securing Personal Information and the OIPC's PrivacyRight webinar on Security Safeguards.

3.5 Video Surveillance & FRT

3.5.1 Video Surveillance

All 30 liquor and cannabis retailers indicated that they have video surveillance in their retail stores. Of the 10 retailers who submitted written privacy policies for review, five (two liquor, three cannabis) policies mentioned collection of personal information via video surveillance or the use of video surveillance in general.

Retailers should either amend their existing privacy policies or draft policies to include the collection of images of individuals via video surveillance, and ensure that security safeguards are extended to surveillance systems as well. Policies should explain, at minimum:

- the purposes for such surveillance;
- when and how monitoring and recording will take place;
- how recorded images may be used and who may access recordings;
- retention periods;
- secure deletion or destruction; and
- how the retailer will secure against unauthorized access or disclosure.

RECOMMENDATION 13

Retailers should draft or amend privacy policies to include the collection and management of personal information via video surveillance.

3.5.2 Notification for Video Surveillance

Retailers are required to provide written notice to advise those entering the retail stores about the collection of personal information via video surveillance. Notices must be posted in an easily viewable location and must indicate (1) that video surveillance is in use and (2) the purposes for collection.

Three of the retailers reported that they did not have notices posted to indicate the use of video surveillance, and one retailer who provided a copy of the notification reported that some of their stores have the signage while others do not. In total, 26 retailers (12 liquor, 15 cannabis) provided a copy of video surveillance notices for review.

Each of the 26 notices contained the first requirement of indicating that video surveillance is in use. However, only nine of the retailers' notices (six from liquor retailers, three cannabis) included the purposes for collection. This means that 21 retailers did not provide adequate notification. Without visible signage pointing to the collection of personal information (i.e., images of individuals) via video surveillance and the purposes for collection, organizations fail to meet the notification requirements of s. 10 of PIPA.

RECOMMENDATION 14

Retailers must post signage at all store entrances to notify individuals of the collection of personal information via video surveillance and the purposes for such collection.

3.5.3 Biometrics & FRT

When asked about the collection and use of biometric information by retailers, four reported the use of temperature scanners or thermometers, one noted the use of an ID card scanner, one utilizes a thumbprint scanner, and one has included FRT as part of its video surveillance system.

Temperature

Four retailers (two liquor, two cannabis) noted that they have temperature scanners or thermometers available in store for employees to screen for symptoms of COVID-19 during the pandemic. Three of these are regular digital thermometers, two are for voluntary staff use if symptomatic, and one is for mandatory use and staff manually record their temperature before they start a shift.

The fourth device is a temperature scanner, MiCovid Cam. The retailer and the posted notification state that the device is mandatory for staff to check their temperature prior to their shift and, as a public service, they offer the voluntary use of the temperature reader for client use. Similarly, both the retailer and the notice note that "this tool is only set to measure temperature. No biometric information or data is obtained, stored or transmitted." The retailer confirmed that the device is not linked to a server and the only function that is turned on is the temperature reader and not any facial recognition or other biometric measurement.

ID cards

One retailer reported their organization's use of an ID scanning system called Patronscan though noted that the FRT component of the device is not in use. It is likely that other retailers are using ID scanners but did not report this if they were unaware of the potential for FRT within the device or have not enacted the function within their system.

Patronscan takes and scans photos of an individual and their ID card. According to its website, Patronscan can compare data points from the images collect and other information on the ID card to determine the card's authenticity. The system facilitates retailers' visual comparisons of photos taken and can assist the retailer in asking key questions to solicit information to verify that the ID card does belong to the individual using it.

In some limited circumstances with strong evidence of a demonstrated need, individual identification scanning systems may be authorized for the purposes of identifying individuals who pose a safety risk to staff or patrons. In that event, personal information of individuals who do not pose a safety risk must not be retained and must be deleted regularly.

Thumbprints

One retailer's payroll program utilizes a thumbprint scanner for employees to clock in and out at the beginning and end of their shifts. To comply with PIPA, retailers must be able to demonstrate that the collection of employee personal information by means of a thumbprint or fingerprint scanner is reasonable for the purposes of managing the employment relationship and that the collection and use will be limited to that purpose.

Retailers are also required to ensure their security arrangements protect this type of personal information, considering its sensitivity, from any unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks to comply with PIPA.

Faceprints

One liquor retailer reported use of the FRT software FaceFirst by SilverPoint in at least one of their stores. The retailer cited the safety of their locations and property as the purpose(s) for collecting biometric information. The notification indicating that the premises are being recorded does not include mention of FRT. The signage states:

> CAMERAS IN USE
> FOR YOUR PROTECTION AND OURS
> These premises are protected by closed circuit television. For the protection of our valued customers and employees, images are recorded for the purpose of crime prevention and public safety. We may also share these images with law enforcement and other security organizations to provide the evidence we need to prosecute criminal offences.
> 24 Hour Video Recording
> Contact <*security vendor*>

The privacy of individuals must be balanced with the information needs of an organization and the collection of personal information must be what a reasonable person would consider appropriate in the circumstances. Due to the immutable nature of facial biometrics and the sensitivity around facial vectors created via FRT, and considering that the video surveillance system will capture images of anyone entering the store, the loss of privacy for a number of individuals not involved in criminal offences is not proportional to the benefit gained from potentially assisting law enforcement to identify a select few.

In addition, the collection of biometric information and the sensitivity of such information generally requires *express* consent.[17] While liquor and cannabis retailers may be authorized to collect, use and disclose personal information via video surveillance, the collection, use and disclosure of biometric information is a new and distinct collection that is separate from video surveillance. Due to the sensitive nature of such biometric information, organizations need to have clear authorization for such collection, use or disclosure. As such authorization is not apparent, unless there are exceptional circumstances to consider, BC liquor and cannabis retailers are not authorized to use FRT.

RECOMMENDATION 15
Retailers should immediately stop using FRT.

For further information on video surveillance, see the joint guidance document Guidelines for Overt Video Surveillance in the Private Sector. For information on privacy concerns related to facial recognition and other biometrics, please see the Office of the Privacy Commissioner of Canada's guidance on Data at Your Fingertips Biometrics and the Challenges to Privacy and Automated Facial Recognition in the Public and Private Sectors.

[17] See Joint investigation of Clearview AI, 2021 CanLII 9227 (PCC), paras 38. https://canlii.ca/t/jd55x.

3.6 Retail Websites

3.6.1 Collection of personal information on retail websites

All of the sampled liquor and cannabis retailers maintain a website. On their websites, retailers advertise their company and products and allow individuals to:

- arrange for purchase pick-up, mail order or delivery;[18]
- sign into membership accounts or check rewards;
- opt in to receive a newsletter;
- apply for jobs; or
- contact the company.

Each of these online activities have forms that collect personal information. In addition, websites may also collect web browser information, information submitted in a search, internet protocol (IP) addresses, and so on. Some websites also place cookies (whether their own or from third parties) that may, for example, track and document websites that individuals visited before or after visiting retailers' website.

The types of personal information different retailers overtly collect online directly from customers include:

- contact information (name, email, address, phone number);
- demographics (age or date of birth);
- financial information (credit card numbers);
- member login credentials (member number, account verification using Google, Facebook or Apple profiles);
- purchase/order selection or history;
- work history (cover letters and resumes for job applications);
- education history (highest level obtained, degree/diploma received, industry training certificates or designations);
- open fields to provide additional information;
- Serving it Right certificate number; and
- reward systems (airmiles or retailer reward – liquor retailers only).

[18] At the time of the review, cannabis retailers were not permitted to utilize delivery options or mail order options. Customers could order and pay online but had to pick up in-store. With the pending advent of delivery, anticipated for later 2021, the impact for personal information collection is that delivery drivers will need an individuals' addresses and will have to check the individuals' identification to ensure age requirements are met and to verify that the individual who ordered is the individual receiving the delivery.

The OIPC recommends that retailers who utilize online ordering, online payment processing, or open fields forms (such as on "contact us" pages or for some aspects of education history) limit personal information they collect online and ensure appropriate security for transmission of that information.

RECOMMENDATION 16

Retailers should limit their collection of personal information online and ensure reasonable and effective security considering the sensitivity of the information.

3.6.2 Notification and consent online

As noted, the purposes for retailers' collection of personal information via retailer websites is, in most cases, obvious to a reasonable person and is collected overtly and directly from the individual. Examples include providing an email address for contact purposes, a credit card number for purchasing, or a home address for delivery. In other cases, the collection of personal information may not be overt and the purposes may not be obvious. Examples include additional personal information collected or disclosed when an individual uses social media login credentials (such as Google, Facebook or Apple)[19] to login to their retail membership account; or the collection of computer browser information, IP addresses, or browsing history.

PIPA requires organizations to notify individuals about the purposes for collection on or before collecting personal information unless the purpose is obvious and the individual voluntarily provides their information for that purpose.[20] This means organizations should be notifying individuals prior to collecting personal information online where the purposes for collection are not obvious.

Providing information about the collection and the purposes for such is not sufficient when the notice is contained only within a privacy policy that may be several clicks or links away from the page or tab where the information is collected. Best practice is to clearly notify patrons about the collection and the purposes for such on the first page or instance where that personal information is collected.

[19] When customers login using their Google, Facebook or Apple accounts, these third-party accounts will often provide the customer's name, profile and cover photos, email address, and Apple ID.
[20] For clarification of legislative requirements and further information, see *Guidelines for Online Consent* https://www.oipc.bc.ca/guidance-documents/1638 and Practical Suggestions for your *Organization's Website Privacy Policy* https://www.oipc.bc.ca/guidance-documents/1561.

RECOMMENDATION 17

Retailers must notify individuals in clear terms of the purposes for which they are collecting personal information online.

3.6.3 Website privacy policies

Many retailers (19 of 30) had a privacy policy available on their website, specific to the personal information they collect online and in a reasonably easy-to-find location.

Of the 19 web-based privacy policies, nine policies were missing several elements of a privacy policy, five policies contained roughly half of the elements, and five policies contained most essential aspects. With this, only 5 of 30 retailers had reasonably fulsome online privacy policies. See Table 3 for detail.

TABLE 3 THE NUMBER OF RETAILERS WITH ELEMENTS OF AN ONLINE PRIVACY POLICY

	Liquor Retailers	Cannabis Retailers
Online Privacy Policies	10 of 15	9 of 15
1. Accountability		
- Compliance with PIPA BC[21]	1	1
- Define PI consistent with PIPA	9	5
2. Purpose & Limits to Collection		
- Purpose for collection	8	8
- Limits to collection	8	6
- Description of PI collected	8	8
3. Consent		
- Consent Required for Collection	9	4
- How Consent will be Obtained	7	4
- Right to Withdraw Consent	4	1
4. Disclosure of PI	8	6
5. Retention & Disposal	7	3
6. Accuracy & Correcting PI	6	4
7. Safeguards	8	4

[21] An additional four retailers pointed to BC's public sector *Freedom of Information & Protection of Privacy Act* (FIPPA) instead of the private sector PIPA, and one additional retailer pointed to Alberta's PIPA in their online privacy policy.

- Administrative, Physical or Technological	8	4
- Breach Response Process	1	1
8. Request Access to Own PI	6	4
9. Right to and How to Complain	2	1
10. Openness		
- Contact info for Privacy Officer	3	5
- Contact BC OIPC	1	0

Considering that retail websites are increasingly one of the main avenues through which individuals interact with an organization (particularly over the past year during the COVID-19 pandemic), websites have become an essential location for organizations to communicate with their customers. When online ordering or purchase transactions are among the top methods through which a retail organization operates, it is crucial for the organization to provide transparent information about its personal information management practices in the form of fulsome online privacy policies.

RECOMMENDATION 18

Retailers should post privacy policies online that detail the collection, use, and disclosure of personal information through the website (including device identifiers).

Please see *Guidelines for Online Consent* and *Practical Suggestions for your Organization's Website Privacy Policy.*

4 SUMMARY OF RECOMMENDATIONS

1. Retailers should ensure adequate funding and resources for effective privacy management programs.
2. Retailers without privacy officers must immediately designate one or more individuals to be responsible for ensuring the organization complies with PIPA.
3. Retailers should develop and maintain an inventory of all types of personal information they collect, the purposes for collection, where the information is stored, and its sensitivity.
4. Retailers must develop and maintain policies and practices necessary to meet the obligations under PIPA.
5. Retailers should provide mandatory privacy training and education for all staff, managers, contractors and others who may access the personal information the organization collects.

6. Retailers should ensure that all staff, managers, contractors and others who may access the personal information review the privacy policies and sign a confidentiality agreement.
7. Retailers should establish, document, and communicate clear breach reporting and response processes.
8. Retailers should ensure written contracts and information sharing agreements are in place and express expectations for privacy protection.
9. Retailers should conduct regular risk assessment and compliance monitoring activities and mitigate risks to personal information privacy and security.
10. Retailers should develop and document an annual review plan that details how they will monitor and assess the effectiveness of their overall privacy management program.
11. Retailers should formulate and implement a schedule for retention of personal information that complies with s. 35, and securely destroy or remove the means by which the personal information can be associated with particular individuals in accordance with the retention schedule.
12. Retailers should review administrative, physical, and technological safeguards and ensure they are reasonable and effective, considering the type and sensitivity of personal information their organization collects.
13. Retailers should draft or amend privacy policies to include the collection and management of personal information via video surveillance.
14. Retailers must post signage at all store entrances to notify individuals of the collection of personal information via video surveillance and the purposes for such collection.
15. Retailers should immediately stop using FRT.
16. Retailers should limit their collection of personal information online and ensure reasonable and effective security considering the sensitivity of the information.
17. Retailers must notify individuals in clear terms of the purposes for which they are collecting personal information online.
18. Retailers should post privacy policies online that detail the collection, use, and disclosure of personal information through the website (including device identifiers).

5 CONCLUSION

All private sector licensed liquor and cannabis retailers collect a certain amount of personal information from employees, customers, or others who may enter their retail premises. Most of the retailers also collect personal information online. These collections can include, for example, receiving employment applications containing work history, manually checking a customer's ID to verify their age, capturing their image via video surveillance and, in at least one instance, creating a biometric measurement of customers' facial features.

Findings revealed that few retailers maintained adequate privacy management programs or documented privacy policies. Without these foundational pieces, it becomes clear that private sector liquor and cannabis retailers in BC would benefit from assistance in establishing and documenting effective privacy programs and policies. Relevant OIPC guidance and other resources have been identified throughout this report. There may also be a role for government agencies, such as the LCRB, or for membership organizations like Able BC or ACCRESS, to provide further information about retailers' obligations under PIPA, increase awareness of privacy management, and possibly work with retailers to create or customize privacy management programs and policies.

BC's licensed private sector liquor and cannabis retailers are authorized to collect personal information via video surveillance with implied consent or as authorized by law but must ensure effective safeguards are in place to protect this information and need to ensure signage meets the notification requirements under PIPA. For retailers using or considering the purchase of equipment that is capable of measuring biometrics, they must ensure they have appropriate legal authorization to collect that type of personal information. Even with authorization, retailers should question the impact that this use of technology may have on employee and customer trust.

Individual reports will be provided to the retailers involved in this review. Each individual report contains specific recommendations for their organization and will help guide each retailer in implementing a privacy management program that meets the legislation and guidelines. The OIPC will follow-up on retailers' implementation of the recommendations in six months.

Each of the recommendations from the individual reports have been included in this aggregate copy for the benefit of other liquor and cannabis retailers to better understand their obligations under PIPA, and for other organizations who may be establishing their own privacy management programs.

6 ACKNOWLEDGEMENTS

I sincerely thank the retailers who contributed to this review by providing policies and making themselves available for interview.

I would also like to thank Kaylie Ingram, Compliance Auditor and Tanya Allen, Director of Audit and Systemic Reviews for conducting this compliance review and drafting this report.

June 22, 2021

ORIGINAL SIGNED BY

Michael McEvoy
Information and Privacy Commissioner for British Columbia

7 APPENDIX: RESOURCES

Office of the Information & Privacy Commissioner for BC Guidance

Developing a privacy policy under PIPA. Mar 2019.
https://www.oipc.bc.ca/guidance-documents/2286

Protecting personal information: Cannabis transactions. Oct 2018.
https://www.oipc.bc.ca/guidance-documents/2248

Guidance Document: Information Sharing Agreements. Sep 2017.
https://www.oipc.bc.ca/resources/guidance-documents/

Practical Suggestions for your Organization's Website's Privacy Policy. Aug 2013.
https://www.oipc.bc.ca/guidance-documents/1561

Privacy Breaches: Tools and Resources. Apr 2012.
https://www.oipc.bc.ca/guidance-documents/1428

A Guide to BC Personal Information Protection Act. Apr 2012.
https://www.oipc.bc.ca/guidance-documents/1438

Office of the Information & Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada and Office of the Information & Privacy Commissioner for BC Joint Guidance

Securing personal information: A self-assessment for public bodies and organizations. Oct 2020.
www.oipc.bc.ca/guidance-documents/1439

Guidelines for Online Consent. May 2014.
www.oipc.bc.ca/guidance-documents/1638

Getting Accountability Right with a Privacy Management Program. Apr 2012.
www.oipc.bc.ca/guidance-documents/1435

Guidelines for Overt Video Surveillance in the Private Sector. Mar 2008.
www.oipc.bc.ca/guidance-documents/1453

Office of the Privacy Commissioner of Canada Guidance

Automated Facial Recognition in the Public and Private Sectors. Mar 2013.
www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303

Data at Your Fingertips Biometrics and the Challenges to Privacy. Feb 2011.
www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102
(Currently being updated.)

Office of the Information & Privacy Commissioner for BC PrivacyRight Webinars

10 basic obligations under PIPA. Feb 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-1/

Privacy Management Programs. Mar 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-2/

How to write a privacy policy. Mar 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-2b/

Authority to collect, use, and disclose personal information. Apr 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-3/

Understanding consent and notification. May 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-4/

Security safeguards. Jun 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-5/

Using and disclosing personal information. Jul 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-6/

How to handle access requests and complaints. Aug 2019
www.oipc.bc.ca/privacyright/webinars/webinar-7/

Managing privacy breaches. Sep 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-8/

Risk Management and Compliance Monitoring. Oct 2019.
www.oipc.bc.ca/privacyright/webinars/webinar-9/