COMPLIANCE REPORT 22-02

Follow-up review of private liquor and cannabis retailers

JUNE 7, 2022
CANLII CITE: 2022 BCIPC 29
QUICKLAW CITE: [2022] B.C.I.P.C.D. NO. 29

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

When you make an instore or online purchase, chances are you don't think about how the personal information associated with your transaction is protected. In part, this is because we trust businesses to handle and protect our personal information with the same care they handle their valuable inventory and monies collected from customers.

That care is critical when it comes to the personal information gathered by cannabis and liquor retailers. The potential harms resulting from a data breach in this sector are especially acute.

It was for this reason that in 2021 my office reviewed the privacy management programs of the largest retailers in BC. We found that many had a lot of work to do on this important front. Whether the information is collected from customers or staff, we learned that many retailers didn't have the appropriate policies and safeguards in place, while others didn't even realize they collected personal information.

We provided those retailers with individual reports detailing the shortfalls in their policies and practices and recommended ways to help them comply with PIPA. We then followed up several months later, to see how each retailer was doing and where gaps still existed.

I am pleased to report that, by and large, these businesses now have a far better understanding of their responsibility to protect personal information, and have made improvements in all areas of their privacy management programs. Where particular retailers have not yet met all of the recommendations set out, my office will continue to work with them until full compliance has been achieved.

What all retailers can take from this report is that they should not take the trust that customers and employees give them, or their responsibility to appropriately manage personal information, lightly. Instead, they should continuously monitor, evaluate and improve their privacy management programs with the same vigor and urgency towards protecting personal information as they would give to protecting their valuable financial and physical assets.

Michael McEvoy

ORIGINAL SIGNED BY

Information and Privacy Commissioner for BC
June 7, 2022

EXECUTIVE SUMMARY

Privacy management programs set the foundation for organizations to manage the personal information they collect. Liquor and cannabis retailers collect various types of personal information to conduct their business, such as the age or date of birth on drivers' licenses, video images of customers and employees via surveillance systems, credit card information via online purchasing, and employee information for hiring and payroll purposes. Retailers must ensure fulsome privacy management programs are in place to protect such personal information.

During the initial review of 30 liquor and cannabis retailers, auditors found serious gaps. The review found that the retailers largely did not have adequate privacy management programs. Many retailers did not have a privacy officer, privacy policies, an inventory of personal information they collected, or any privacy management training for staff or managers.

The Office of the Information and Privacy Commissioner for BC (OIPC) made 18 recommendations to address the gaps, and provided individual reports to each of the 30 retailers with relevant recommendations. The reports also provided links to guidance documents and other information to assist retailers in improving their privacy management programs, policies, and safeguards. These resources are also listed in the Appendix to this report.

Six months after the release of the report, the OIPC began reviewing the retailers' implementation of the recommendations. As this report details, most of the retailers have implemented the recommendations and, overall, retailers' privacy management programs and compliance with BC personal information privacy laws have improved since the original review.

While there is still room for improvement, by and large retailers have demonstrated positive and meaningful action to further protect personal information. The OIPC will continue to follow-up with retailers until all recommendations are implemented.

1 INTRODUCTION

The OIPC conducts audits, investigations and compliance reviews to assess how effectively private sector organizations protect personal information and comply with provisions under the *Personal Information Protection Act* (PIPA).

In June 2021, under the authority of s. 36 of PIPA, the OIPC published a compliance review of 30 liquor and cannabis retailers.[1] We selected this topic because personal information collected by

[1] https://www.oipc.bc.ca/compliance-reports/3554, published June 2021.

liquor and cannabis retailers can be especially sensitive. In many jurisdictions outside of Canada, cannabis is illegal and certain countries may deny entry to individuals who have purchased cannabis or work in the industry. Additionally, liquor purchases carry their own sensitivities and stigmas that could affect an individual should a breach occur. As such, adequate privacy management is a critical component for liquor and cannabis retailers to protect the personal information they collect.

The review focused on retailers' privacy management programs, privacy policies, and the collection and safeguarding of personal information. In addition, the review examined retailers' use of video surveillance and whether they employ facial recognition technology. The OIPC made 18 recommendations to liquor and cannabis retailers to help them establish fulsome privacy management programs that meet BC's legislation and guidelines.

Six months later, the OIPC began its follow-up with the retailers on their implementation of the recommendations. This follow-up report highlights the retailers' progress.

The original review found that most liquor and cannabis retailers did not have adequate privacy management programs. The 18 recommendations OIPC made to liquor and cannabis retailers included:

1. Ensure adequate **funding and resources** for effective privacy management programs.
2. Immediately designate a **privacy officer** or someone to be responsible for ensuring PIPA compliance.
3. Develop and maintain a **personal information inventory** of all types of personal information they collect, the purposes for collection, where the information is stored, and its sensitivity.
4. Develop and maintain **written privacy policies** and practices necessary to meet the obligations under PIPA.
5. Provide **mandatory privacy training** and education for all staff, managers and contractors.
6. Ensure that all staff, managers and contractors review privacy policies and sign **confidentiality agreements.**
7. Establish, document, and communicate clear **breach response processes**.
8. Ensure written contracts and information sharing agreements with **service providers** are in place and express expectations for privacy protection.
9. Conduct regular **risk assessment** and compliance monitoring activities and mitigate risks to personal information privacy and security.
10. Develop and document an annual **review and revision** of their overall privacy management program.

11. Formulate a **retention schedule** and securely destroy personal information in accordance with that schedule.
12. Review administrative, physical, and technological **security safeguards** and ensure they are reasonable and effective, considering the type and sensitivity of personal information.
13. Amend **video surveillance policies** to include management of personal information collected via video surveillance.
14. Post signage at all store entrances to notify individuals of the collection of personal information via video surveillance and the purposes for such collection (**notification for video surveillance**).
15. Stop using **facial recognition technology**.
16. Limit **collection of personal information on retail websites** and ensure reasonable and effective security.
17. Notify individuals of the purposes for which they are collecting personal information online (**notification and consent online**).
18. Post **website privacy policies** online that detail the collection, use, and disclosure of personal information through the website.[2]

At the time of publishing the original review, the OIPC also provided individual reports to each of the 30 retailers involved in the review. These reports showed a summary of results and recommendations specific to each retailer, and notified retailers that the OIPC would follow-up on implementation of the recommendations in six months.

In January 2022, the OIPC requested an update from all (now 29[3]) retailers regarding their implementation of the specific recommendations. In addition to their written responses, the OIPC requested retailers provide supporting documentation such as updated privacy policies, personal information inventories, breach reporting processes, staff training materials, video surveillance polices, photos of amended signage, and updated retailer website policies.

Auditors reviewed the retailer submissions and, where provided, used the documents to substantiate retailers' statements. Where recommendations had yet to be fully implemented, auditors requested and reviewed retailers' plans for accomplishing the activities.

This follow-up report contains observations on the 29 retailers' implementation of the recommendations.

[2] Please see the published review for the full wording of each recommendation.
[3] One of the retailers originally involved in the review sold its business to another retailer who also happened to be part of the original review, so follow-up commenced with 29 retailers, as opposed to 30.

2 FINDINGS

The OIPC provided a varied number of recommendations to each of the 29 retailers, based on gaps auditors found in each retailers' privacy management program. To date, eight of the 29 retailers have fully implemented all of their applicable recommendations. The remaining 21 retailers have between one and 16 recommendations (average of four each) left to implement.

Overall, across all 29 retailers, 70% of the recommendations have been fully implemented and 22% have been partially implemented. In this context, partially implemented means that retailers had commenced and made some progress to incorporate the recommendation(s) into their privacy management program.

At the time of this follow-up, retailers had yet to start work on implementing 8% of the recommendations. For these recommendations, most retailers have documented how they intend to move forward and their anticipated timeline for implementation. The OIPC will continue to track progress made on implementing all remaining recommendations. Table 1 (next page) provides a count of how many retailers implemented each recommendation.

Privacy management programs help to foster respect for personal information and help organizations to meet their legislative obligations under PIPA. As shown in Table 1, auditors identified that the retailers largely accepted and implemented the recommendations to improve their privacy management programs.

There were some noticeable differences between liquor and cannabis retailers regarding the extent of implementation of certain recommendations. Specifically, auditors found that liquor retailers appeared more likely to have:

- a designated a privacy officer;
- written privacy policies; and
- expectations for privacy protection included in contracts.

It is particularly important that cannabis retailers designate privacy officers, develop policies, and strengthen their overall privacy management programs. As mentioned above, a breach for a cannabis retail organization can have more negative implications for individuals compared to other types of organizations.

TABLE 1 – IMPLEMENTATION OF RECOMMENDATIONS				
	Number of Liquor and Cannabis Retailers			
	Fully Implemented	Implementation Ongoing	Not Implemented	**Total # of Retailers Given this Recommendation**
PRIVACY MANAGEMENT PROGRAM				
1. **Funding & Resources**	15	1	3	**19**
2. **Privacy Officer**	13	2	4	**19**
3. **Personal Information Inventory**	20	5	2	**27**
4. **Written Privacy Policies**	13	9	-	**22**
5. **Mandatory Privacy Training**	19	5	3	**27**
6. **Confidentiality Agreements**	15	2	1	**18**
7. **Breach Response Processes**	21	2	4	**27**
8. **Service Provider Management**	12	5	4	**21**
9. **Risk Assessment**	8	6	-	**14**
10. **Review and Revision**	9	8	2	**19**
PRIVACY POLICIES & PRACTICES				
11. **Retention Schedule**	22	6	1	**29**
SECURITY SAFEGUARDS				
12. **Security Safeguards**	21	4	3	**28**
VIDEO SURVEILLANCE & FACIAL RECOGNITION TECHNOLOGY (FRT)				
13. **Video Surveillance Policies**	18	4	2	**24**
14. **Notification for Video Surveillance**	12	11	1	**24**
15. **Facial Recognition Technology**	1	-	-	**1**
RETAIL WEBSITES				
16. **Collection of Personal Information on Retail Websites**	7	2	-	**9**
17. **Notification and Consent Online**	15	2	-	**17**
18. **Website Privacy Policies**	17	5	1	**23**

Across the retailers, auditors also observed that some missed particular aspects of a recommendation during implementation. Examples of this and other "lessons learned" during this follow up included:

- Some retailers still did not understand what constitutes personal information, nor their obligation to ensure all types of personal information are accounted for in their privacy management program. Liquor and cannabis retailers collect a lot personal information about customers, employees and others, often including:
    - images of individuals collected via video surveillance;
    - customer dates of birth from ID cards during age verification;
    - customer contact information, credit card information and purchase history;
    - customer computer information through online orders; and
    - employee personal contact information, work history, security clearance, payroll and tax information, and health information.
- As a result of not understanding what constitutes personal information, some retailers failed to capture both employee and customer personal information in their personal information inventories, privacy policies, and retention schedules. It's important that organizations account for all types of personal information they may collect to ensure they have reasonable security arrangements in place.
- Some privacy policies lacked key components. Privacy policies should cover all aspects in the life cycle of managing personal information, from ensuring collection of personal information is limited to what is authorized by PIPA and collected with appropriate notification and consent; to limiting how the personal information is used or disclosed, illustrating how the information will be safeguarded; and storing the information only as long as needed or required by PIPA. Privacy policies should also detail how a person may withdraw consent, access their own personal information, and raise any concerns they may have about the organization's handling of personal information. OIPC guidance on Developing a Privacy Policy under PIPA further defines these key components.
- Some retailers need to do more to ensure that their policies and security safeguards keep pace with changes in information security standards, and that staff receive privacy training that details the sensitivity of personal information in the context of liquor and cannabis retail.
- Some retailers' risk assessment plans included physical safeguards but not administrative or technological safeguards. Retailers that do not implement relevant administrative, physical and technological safeguards or do not monitor the effectiveness of them fail to meet their legal obligations to make reasonable security arrangements to prevent authorized access, collection, use, disclosure, copying or similar risks.
- With video surveillance, retailers need to consider and limit who can access video recordings and still images taken from surveillance videos. Unauthorized disclosure of

such information (such as making images extracted from surveillance videos publicly available) can create a serious breach. Auditors found that some retailers also do not have a process for documenting or logging occasions where the video surveillance has been used or disclosed.

- In addition, many retailers did not account for personal information collected by video surveillance in their privacy policies or failed to explain:
    - the purposes for such surveillance;
    - 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.
- Auditors also found that, while most retailers had posted signage outside of their retail stores to notify individuals of the collection of personal information via video surveillance, this signage often did not inform individuals of the purposes for collection.

As mentioned above, eight of 29 retailers have finished implementing all recommendations, while 21 retailers are in various stages of implementing the recommendations. Of the recommendations provided by the OIPC, retailers have implemented 70% of them, partially implemented 22%, and have not yet started work on implementing 8% of the recommendations.

Auditors found that retailers who had implemented the fewest recommendations also failed to designate a privacy officer or someone responsible for ensuring PIPA compliance. Not surprisingly, these retailers were also likely to have reported that they did not have adequate funding or resources for an effective privacy management program. Support from executive is critical for any organization's privacy management program to be adequate and effective. These retailers have the most work to do to ensure they comply with their legislated responsibilities under PIPA, and the OIPC will continue to work with them until a privacy officer is in place and all recommendations have been satisfactorily implemented.

3 CONCLUSION

All licensed private sector liquor and cannabis retailers collect personal information from employees, customers, or others who may enter their retail premises or online. Liquor and cannabis retailers are legally obligated to ensure that such collection, use, retention and disclosure of personal information complies with PIPA.

The initial 2021 review found that few retailers maintained adequate privacy management programs or documented privacy policies. This follow-up showed that most retailers have accepted and made significant strides toward implementing the OIPC's recommendations and,

thereby, have improved their overall privacy management and protection of personal information.

For other retailers, the work continues. The OIPC has communicated with these retailers concerning their failure to meet their obligations under PIPA and to set timelines for implementing the recommendations to come into compliance with the legislation. The OIPC will continue to track progress made for any outstanding recommendations.

The results of the review and this follow-up are broadly reflective of BC's licensed private liquor and cannabis retail sector. Compliance reviews such as this one provide learning opportunities for not only for the organizations involved but for other organizations generally, to help them understand their obligations for protecting personal information. The review and the continued follow-up with retailers to ensure all recommendations are implemented have a broad impact on the liquor and cannabis retail sector in BC, impacting thousands of customers, employees and others who trust that their personal information is handled appropriately.

Licensed private sector liquor and cannabis retailers in BC who were not involved in this review are encouraged to read the original published review, along with the lessons learned from this follow-up. All retailers should assess their own privacy management programs to ensure they have implemented the 18 recommendations and are compliant with PIPA.

4 ACKNOWLEDGEMENTS

I thank the liquor and cannabis retailers who contributed to this follow-up review by providing updates on their implementation of the recommendations, along with relevant documents and materials. I commend the retailers who have done the work to ensure their compliance with BC's legislative requirements.

I would also like to thank Gary Freeburn, Compliance Auditor and Tanya Allen, Director of Audit and Systemic Reviews, for conducting this compliance review follow-up and drafting this report.

June 7, 2022

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

5 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/