OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
Prince Edward Island

Investigation Report No. PP-20-001

Re: Cannabis Management Corporation

Prince Edward Island Information and Privacy Commissioner
Karen A. Rose

April 22, 2020

Summary: The Commissioner commenced an investigation of Cannabis PEI, following public concerns regarding electronic scanning of customers' identification cards. Although Cannabis PEI halted the process of scanning identifications, the Commissioner examined their practices relating to personal information.

In their in-person retail setting, the Commissioner found that Cannabis PEI collects personal information of individuals, including video images, and basic personal information for incident reports, complaints, inquiries, and merchandise returns. The Commissioner found that Cannabis PEI is authorized to collect, use and disclose such personal information for the limited purposes reported. With respect to video surveillance, the Commissioner made recommendations to Cannabis PEI regarding their obligation to notify the public of their purpose, authority, and contact information.

In their online setting, the Commissioner found that Cannabis PEI collects personal information of individuals, including for order and delivery purposes. The Commissioner found that Cannabis PEI is authorized to

collect, use and disclose such personal information for the limited purposes reported.

The Commissioner also examined the security arrangements made by Cannabis PEI to protect the personal information in their custody and control. The Commissioner found, based on the available information, that Cannabis PEI is using reasonable security measures to protect personal information. However, as the security of online sales and electronic databases is an ever-evolving risk, the Commissioner recommended that Cannabis PEI incorporate proactive measures, including periodic and comprehensive reviews and testing of their security measures.

Statutes considered: *Cannabis Control Act,* RSPEI 1988, c C-1.2

Cannabis Control Regulations, PEI Reg EC575/18

Cannabis Act, SC 2018 c. 6, 7(b)

Cannabis Management Corporation Act, RSPEI 1988, c C-1.3, ss. 20(b)

Cannabis Management Corporation Regulations, PEI Reg EC460/18, ss. 4(3), 7(2)

Freedom of Information and Protection of Privacy Act, RSPEI, c F-15.01, sections 1(i), 31, 32, 35, 36, 37, 50(1)(a)

Decisions cited: BC Order P10-01, *Re: Host International of Canada Ltd*, 2010 BCIPC 7 (CanLII)

AB Order H2007-002, *Drugstore Pharmacy, Real Canadian Superstore,* 2008 CanLII 88797

Investigation Report IR-16-001, *Re: Department of Justice and Public Safety*, 2016 CanLII 23239 (PE IPC)

Investigation Report F11-01, *Re: Investigation into a Privacy Breach of Customers' Personal Information by the British Columbia Lottery Corporation*, 2011 BCIPC 6 (CanLII)

Also considered: *Reviewing the Return Policies of the Liquor Control Board of Ontario; Privacy Investigation, Report PC-7-100, and A Review of the Literature Relating to Fraudulent Returns: Practices used by Retailers to Combat Fraud.* Ontario Information and Privacy Commissioner, January 15, 2009. https://www.ipc.on.ca/wp-content/uploads/2016/11/pc07-100-lcbo.pdf

A society in transition, an industry ready to bloom - 2018 cannabis report, Deloitte. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/consulting/ca-cannabis-2018-report-en.PDF

I. BACKGROUND

[1] The sale of cannabis became legal in Canada on October 21, 2018. In Prince Edward Island, Cannabis Management Corporation ("the Public Body") is responsible for the sale of cannabis to the public. A concern which arose during the initial days of legalization was the Public Body's requirement that customers provide government-issued identification, which the Public Body electronically scanned. The Office of the Information and Privacy Commissioner ("the Commissioner") commenced an investigation, pursuant to clause 50(1)(a) of the *Freedom of Information and Protection of Privacy Act ("*the *FOIPP Act"),* which states, in part:

> 50(1) In addition to the Commissioner's functions under Part IV, with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may
>
> > (a) conduct investigations to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records …
> > . . .

[2] Within a few days of opening retail outlets, the Public Body changed their process, and ceased scanning identification cards. The Public Body advised the Commissioner that they have no plans to re-introduce ID scanners. However, in the event that they consider changing their decision, they are willing to conduct a privacy impact assessment, an in-depth analysis to identify and address information privacy risks before embarking on new policies or initiatives.

[3] Although cannabis use is now legal in Canada, personal information associated with cannabis purchases is sensitive. Cannabis use may still carry a negative stigma within Canada, and it remains illegal in other countries. Negative repercussions of disclosure of information regarding an individual's cannabis use may include denial of entry into countries where cannabis is illegal. Due to the sensitivity of such personal information, the Commissioner decided to continue the investigation into the policies and procedures of the Public Body.

[4] The Public Body has two sales models: brick and mortar retail stores, and an online store. The Commissioner gathered information with respect to the collection, use, disclosure, and protection of personal information in both types of outlets, to determine whether the Public Body's activities are compliant with their obligations under the *FOIPP Act*.

II. ISSUES

[5] The Commissioner reviewed four key issues in the analysis of the Public Body's information handling practices:

> Issue 1: Does the Public Body collect personal information and, if so, is their collection authorized by the *FOIPP Act*?

Issue 2: Does the Public Body use personal information and, if so, are all uses authorized by the *FOIPP Act*?

Issue 3: Does the Public Body disclose personal information, and if so, are these disclosures authorized by the *FOIPP Act*?

Issue 4: Has the Public Body made reasonable security arrangements to protect the personal information in their custody or control against such risks as unauthorized access, collection, use, disclosure, disposal or destruction?

III. ANALYSIS

[6] In this Report, I will be examining the following information, to determine whether the Public Body's information practices comply with the provisions of the *FOIPP Act*:

a. Information related to the retail setting, including video surveillance, inspection of identification, point of sale payments, and employees' incident reports of an alleged crime;
b. Information related to inquiries and complaints;
c. Information related to returned products;
d. Information related to accessing the Public Body's website;
e. Information related to online order placement; and
f. Information related to delivery of online orders.

Issues 1, 2 and 3: Collection, Use and Disclosure

[7] I will describe each type of personal information the Public Body collects, first in the retail setting, and then in the online setting. In each instance I will review whether the Public Body has authority to:

a. collect the personal information under sections 31 or 32 of the *FOIPP Act;*
b. use the personal information under section 36 of the *FOIPP Act*; and
c. disclose the personal information under section 37 of the *FOIPP Act*.

[8] Subsection 1(i) of the *FOIPP Act* defines "personal information" quite broadly, as recorded information about an identifiable individual. The definition then lists several types of information that are personal information, such as an individual's name, home or business address, or home or business telephone number. Personal information also includes an identifying number assigned to the individual.

Collection

[9] The authority for a public body to collect personal information is found at section 31 of the *FOIPP Act*, which states:

> Purpose of collection of information
> 31. No personal information may be collected by or for a public body unless
> (a) the collection of that information is expressly authorized by or under an enactment of Prince Edward Island or Canada;
> (b) that information is collected for the purposes of law enforcement; or
> (c) that information relates directly to and is necessary for an operating program or activity of the public body.

[10] Subsection 32(1) of the *FOIPP Act* requires a public body to collect personal information directly, unless an exception to this requirement applies. Section 32 states, in part:

> 32. (1) A public body shall collect personal information directly from the individual the information is about unless
> (a) another method of collection is authorized by
> (i) that individual,
> . . .
> (c) the information is collected for the purpose of law enforcement;
> . . .

[11] Subsection 32(2) of the *FOIPP Act* requires that public bodies notify individuals when they are collecting personal information:

> Right to be informed
> 32(2) A public body that collects personal information that is required by subsection (1) to be collected directly from the individual the information is about shall inform the individual of
> (a) the purpose for which the information is collected;
> (b) the specific legal authority for the collection; and
> (c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

[12] The subsection 32(2) notification must state the purpose for the collection, the legal authority for the collection, and the title, business address and business telephone number of an employee of the public body who can answer the individual's questions about the collection.

Use

[13] Subsection 36(1) of the *FOIPP Act* includes a short list of authorized uses of personal information. The most common clause relied upon by public bodies is clause 36(1)(a), which states:

> 36. Use of personal information
> (1) A public body may use personal information only
> (a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose;

Disclosure

[14] Section 37 of the *FOIPP Act* sets out circumstances under which a public body may disclose personal information. The information provided by the Public Body raises clause 37(1)(o) of the *FOIPP Act*:

Disclosure of personal information
37(1) A public body may disclose personal information only
…
(o) to a public body or a law enforcement agency in Canada to assist in an investigation
(i) undertaken with a view to a law enforcement proceeding, or
(ii) from which a law enforcement proceeding is likely to result;

[15] Subsection 1(e) of the FOIPP Act defines "law enforcement" as follows:

1 (e) "law enforcement" means
(i) policing, including criminal intelligence operations,
(ii) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or
(iii) proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings, or by another body to which the results of the proceedings are refer

[16] The Public Body does not disclose the personal information it collects, except in limited and defined circumstances, including for law enforcement purposes. The Public Body also advises as follows:

> . . . personal information collected by CMC is disclosed to third parties in limited circumstances. In the case of online sales, customers accept the CMC's terms and conditions, one of which involves disclosure to third parties involved in order processing and delivery. CMC would also be compelled to disclose where required by law. ["CMC" refers to Cannabis Management Corporation, which is the Public Body]

[17] In those circumstances where the Public Body has indicated they may disclose personal information to third parties, I will review whether such disclosure is authorized by section 37 of the *FOIPP Act*.

Video surveillance

[18] The Public Body has security cameras in both the interior and exterior of their retail stores. Video images capture personal information about individuals through their activities. An individual may be identifiable by their characteristics, such as the image of their face, hair, height and size, and/or clothing. Among other types of personal information, the video images include the personal information that the individual was at a cannabis retail store, and whether they purchased anything. I find that the video images are personal information of the individuals they depict.

[19] The Public Body relies on subsection 31(c) of the *FOIPP Act,* that the collected video information relates directly to and is necessary for an operating program or activity of the Public Body. The Public Body submits that they collect video images for the purpose of loss prevention and security. The Public Body submits:

> Security cameras are, in the CMC's view, necessary and reasonably related to its operating activities and similar to security found at many private sector retail establishments.

[20] I accept that loss prevention and security of the premises, staff, and customers at a cannabis retail store are, pursuant to subsection 31(c) of the *FOIPP Act,* operating activities of the Public Body. I will next consider whether the collection of the video images "relates directly to and is necessary for" these activities, as set out in subsection 31(c) of the *FOIPP Act*.

[21] With respect to loss prevention, the Public Body controls entry into the retail area. In addition, given that products are dispensed by staff behind a counter, there is a lower

chance of shoplifting than in other retail settings, as customers are typically not handling the product before they purchase it.

[22] With respect to security of the premises, staff and customers, the retail sale of cannabis is a new landscape in Canada. Although the sale of cannabis is legal, the Public Body notes that prior to legalization cannabis was "a lucrative source of revenue for organized crime". In the months prior to legalization, there were reports of armed robberies of cannabis dispensaries in a neighbouring province. As organized crime is associated with the cannabis market, the association may represent a violence and security risk.

[23] I find that the Public Body's assessment that video surveillance at their retail outlets relates directly to, and is necessary for loss prevention and security, is reasonable. I therefore find that the Public Body's collection of personal information via video surveillance is authorized under subsection 31(c) of the *FOIPP Act*. Further, I find that clause 36(1)(a) of the *FOIPP Act* authorizes the Public Body to use the video for loss prevention and security, as the personal information is used for the same purpose for which it is collected.

[24] With respect to disclosure of personal information collected by video surveillance, the Public Body indicates that disclosure to third parties only occurs where required by law. In their Loss Prevention and Security Manual, "Section 3: Unlawful Activities and Incidents", at page 4, the Public Body advises implicitly, that they will permit a police officer to view a video taken by the Public Body if they request assistance, whether or not the incident under investigation occurred on the Public Body's premises. Also in the manual, "Section 6: Closed Circuit Television (CCTV)", the Public Body notes that Information from the CCTV system may be released to the Director of Corporate Services or to law enforcement personnel. Any additional releases must receive approval from the Director of Corporate Services. The Public Body creates an incident report whenever they permit police services to review the CCTV video.

[25] As disclosure to a law enforcement agency is contemplated by clause 37(1)(o) of the *FOIPP Act*, I find that clause 37(1)(o) of the *FOIPP Act* authorizes the Public Body to disclose video surveillance information to a law enforcement agency, for the purpose of law enforcement.

[26] As noted above, subsection 32(2) of the *FOIPP Act* requires that public bodies notify individuals when they are collecting personal information directly from an individual. I consider video surveillance to be a direct collection of personal information. The notification may be a combination of publicly available policy and signage. If a public body determines that video surveillance is necessary, they must post their notification pursuant to subsection 32(2) of the *FOIPP Act*. During our investigation, the Public Body invited the Commissioner's comments regarding how best to comply with subsection 32(2) of the *FOIPP Act* via their security camera signage.

[27] In the retail setting, the Public Body has signage indicating that video surveillance is occurring. At present, the signs state, "Smile! You're on camera. Security cameras are used in this store. Let us know if you have any questions." The signage does not include all of the information required under subsection 32(2) of the *FOIPP Ac:,* the purpose for the collection; the legal authority for the collection; and the title, business address and business telephone number of an employee of the public body who can answer the individual's questions about the collection. These details are, however, available on the Public Body's website. I recommend that the Public Body amend their signage to either specifically include the subsection 32(2) requirements, or to direct individuals to the policy on surveillance available on the Public Body's website, which includes the subsection 32(2) requirements.

Inspection of an identification card

[28] In Prince Edward Island, it is against the law to sell cannabis to anyone under the age of 19. It is also against the law for a person under the age of 19 to enter or be present in a cannabis retail outlet. To comply with the law, the Public Body may request proof of

age from a person making a purchase, or coming into the store, pursuant to subsection 20(b) of the *Cannabis Management Corporation Act,* RSPEI 1988, c C-1.3, and subsections 4(3) and 7(2) of the *Cannabis Management Corporation Regulations,* PEI Reg EC460/18.

[29] The Public Body's website states on their FAQ page, under the question, "How will you ensure cannabis is sold in a socially responsible way?":

> All customers who choose to shop at a cannabis retail store will be required to present identification, both upon entering the store, and when they finalize their purchase. Preventing sales to anyone under the designated legal purchasing age of 19, and to intoxicated people, is a core focus of PEI Cannabis. All retail staff are well-trained in ID verification and responsible service.

[30] The Public Body does not require every individual to produce identification information upon entering the store. The Public Body also has the following statement at the bottom of their homepage:

> 19+ Only.
> PEI Cannabis currently abides by a Check 30 policy where our retail staff asks for ID from any customers who appear to be under the age of 30.

[31] In the retail model, the Public Body does not always require a purchaser to produce identification when they finalize their purchase. However, if there is any doubt about whether the individual is of eligible age, they may request that the individual confirm their age with an identity document.

[32] The information on a photo identification card, including name, date of birth, ID number, and photo image, is personal information of the identification holder, in accordance with subsection 1(i) of the *FOIPP Act*.

[33] It has been held that viewing, without recording, an individual's driver's license is a collection of personal information [see BC Order P10-01, *Re: Host International of Canada Ltd*, 2010 BCIPC 7 (CanLII), at paragraph 6, and AB Order H2007-002, *Drugstore Pharmacy, Real Canadian Superstore,* 2008 CanLII 88797, at paragraphs 50, 67, 74, and 92]. The Public Body inspects an individual's identification for the purposes of confirming the individual is at least 19 years of age. I find that collecting this personal information is directly related to and necessary to confirm that individuals purchasing cannabis are over the age of 19, and that the Public Body's collection of this personal information is authorized under subsection 31(c) of the *FOIPP Act*.

[34] The Public Body uses the identification card information to assess whether to permit an individual to enter their retail stores, or to make a purchase. Such use is authorized by subsection 36(1)(a) of the *FOIPP Act*, as it is for the purpose it was collected. As the Public Body does not record any personal information from the identification, they are not in a position to disclose personal information. Therefore, it is not necessary for me to address disclosure.

Incident Reports

[35] If an employee of the Public Body suspects that an individual has committed a crime, the Public Body requires the employee to prepare a report describing the incident. If possible, they are also asked to describe the suspect(s), and witness(es). I find that this is a collection of personal information, and that the collection is for the purpose of law enforcement, which is authorized pursuant to subsection 31(b) of the *FOIPP Act*. The definition of "law enforcement" pursuant to subsection 1(e) includes security investigations:

> 1. In this Act
> (e) "law enforcement" means
> . . .
> (ii) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or

> sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or. . .

[36] I am satisfied that, if employees of Public Bodies are recording personal information related to a suspected crime, they are collecting this personal information for the purpose of providing it to a police agency for an investigation. The expression 'security investigation' is not defined in the *FOIPP Act*. However, I accept that it includes an investigation conducted by a public body that is not a police agency, relating to a suspected crime. Further, I am satisfied that the results of the investigation may lead to a penalty or sanction by the courts.

[37] I further find that clause 36(1)(a) of the *FOIPP Act* authorizes the Public Body to use incident reports for law enforcement, as the personal information is used for the same purpose for which it is collected. I also find that clause 37(1)(o) of the *FOIPP Act* authorizes the Public Body to disclose the personal information in the incident reports to a law enforcement agency, for the purpose of law enforcement.

Inquiries and complaints

[38] In the retail setting, if an individual wishes to make an inquiry or a complaint, the Public Body may collect personal information from the inquirer or complainant, such as their name, address, email address, phone number, and the substance of their inquiry or complaint. I find that this is a collection of personal information.

[39] I accept that the collected personal information is related to and is necessary for the Public Body's operations, which includes responding to inquiries or complaints. I find that the Public Body's collection of personal information is authorized under subsection 31(c) of the *FOIPP Act,* and its use is for the purpose for which the information was collected, pursuant to clause 36(1)(a) of the *FOIPP Act*.

[40] The Public Body does not disclose any personal information relating to inquiries or complaints. I therefore provide no analysis relating to disclosure.

Product returns

[41] When a customer returns a product, the Public Body requires that they provide their name, address, email address, phone number, and signature on a form entitled "PEICMC Customer Purchase Return Identification Form". I find that this is personal information. The Public Body has a notice on the form as follows:

> NOTE: By signing this the customer is acknowledging the severity of a fraudulent return, and declares that the product being returned is being returned in good faith. Further, by signing this the customer acknowledges that their personal information will be maintained by the PEICMC for a period of one (1) year to be referenced in various loss prevention efforts to mitigate fraudulent returns. Returns found to be fraudulent in nature will result in the incident being referred to the office of the Attorney General.

[42] The purpose of collecting this personal information is to detect fraudulent returns. The Ontario Office of the Information and Privacy Commissioner conducted a review and produced an investigation report in 2009 on liquor board return policies: *Reviewing the Return Policies of the Liquor Control Board of Ontario; Privacy Investigation Report PC-7-100, and A Review of the Literature Relating to Fraudulent Returns: Practices used by Retailers to Combat Fraud.* The Ontario Commissioner accepted that there are high levels of fraud associated with the return of goods, "in the vicinity of 10%". I accept that fraudulent returns are a challenge to retail operators, and that detecting fraud is an operating activity of the Public Body. I find that collecting this personal information is directly related to and necessary to deter and detect product return fraud, and that the Public Body's collection of personal information is authorized under subsection 31(c) of the *FOIPP Act*. I further find that the Public Body's use of this personal information is for

the purpose for which the information was collected, and is therefore authorized under clause 36(1)(a) of the *FOIPP Act*.

[43] The Public Body did not provide information about disclosure of personal information related to their fraud detection measures. However, I find that clause 37(1)(o) of the *FOIPP Act* would authorize the Public Body to disclose this personal information to the Office of the Attorney General or a law enforcement agency, for the purposes of law enforcement.

Point of sale payments

[44] At the point of sale, when an individual pays by credit or debit, the credit card or debit card information is provided to an outside internet payment processing service through a terminal, similar to many retail interactions. The third party payment processor is authorized to collect the credit or debit information for the Public Body. I find that collecting this personal information is directly related to and necessary to process payments for product, and that the Public Body's collection of this personal information is authorized under subsection 31(c) of the *FOIPP Act*. Further, the Public Body uses the personal information to process the payments, which is for the same purpose it was collected, consistent with clause 36(1)(a) of the *FOIPP Act*.

[45] The Public Body does not store the payor's name or banking information. The only information provided by the internet payment processing service to the Public Body is whether the transaction is accepted or declined, and the last four digits of the credit card or debit card. The Public Body also records what product was sold, the quantity, the date and time of the sale, and the price and taxes. With no identifying information, I find that this is not personal information. As the Public Body is not in a position to disclose personal information from point of sale payments, it is not necessary for me to address disclosure.

Automatic collection of personal information

[46] The Public Body's website collects IP addresses for two separate and distinct purposes: to conduct web analytics and, if required, to determine an individual's identity for law enforcement purposes.

[47] It is common website practice to collect IP addresses to identify unauthorized attempts to change information or damage systems. This practice does not include the collection of names or addresses of visitors to the website.

[48] As an IP address may be used to determine a user's identity, it satisfies the definition of personal information. However, the Public Body advises that they make no effort to identify individuals through their IP addresses, except for law enforcement purposes:

> PEI Cannabis does not use this data to determine your identity unless required to do so as part of an internal investigation or other law enforcement purpose.

[49] The Public Body acknowledges that they automatically collect IP addresses via their website, but they do not retain this information unless for law enforcement purposes. As determined in investigation report IR-16-001, *Re: Department of Justice and Public Safety*, 2016 CanLII 23239 (PE IPC), even if a public body does not retain the original personal information, they may still be collecting it, and are subject to the *FOIPP Act* limitations on the authorized purposes for collection.

[50] I consider monitoring of network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage, to be an operating activity of the Public Body. I also accept that this monitoring relates directly to and is necessary for online sales of cannabis. I find that such a collection of personal information is authorized by section 31 of the *FOIPP Act*.

[51] Web analytics are also a commonly used method to determine useful information such as the pages of the website most commonly accessed, the dates and times most commonly browsed, and the type of web browser used. For web analytics, IP addresses are anonymized so that individuals who browse are not identified in the aggregate information.

[52] If an individual visits the Public Body's website to browse, download or make a purchase, the Public Body's privacy policy advises that they collect the following information automatically:

> **What kind of information is being automatically collected?**
> When you visit the Website to browse, download information or complete a transaction, the following information about your visit will be automatically collected and stored:
> - the Internet Protocol (IP) address and domain name used. The IP address is a numerical identifier assigned either to your internet service provider or directly to your computer. This address can be translated to determine the domain name of your service provider as well as the type of browser and operating system being used;
> - the date, time and duration of your visit; and
> - web pages visited and online applications or services used.

[53] The Public Body advises that they use the above information to create aggregated statistical information related to the following arising from the public's use of their website.

> . . . online visitation as a means to gauge various online uptake metrics (e.g. total visits, etc.), high-level navigational trends (e.g. most visited sites, etc.), and referral sources (e.g. social media links vs website links, etc.)

[54] With respect to statistical and systems performance management, I consider whether collection for this purpose is authorized under subsection 31(c) of the *FOIPP Act*. As noted earlier, to satisfy subsection 31(c) of the *FOIPP Act*, one must identify an

operating program or activity of the Public Body, and assess whether the collected information relates directly to and is necessary for that program or activity.

[55] I accept that online sales of cannabis is an operating activity of the Public Body, and that some form of analysis of the effectiveness of the website relates directly to and is necessary for online sales of cannabis. I further accept that online sales is not a static model, and that ongoing or periodic analysis of the effectiveness of the website is necessary for the operating activity of online sales of cannabis.

[56] Based on the foregoing, I find that the Public Body's automatic collection of IP addresses is authorized under subsection 31(c) of the *FOIPP Act.*

[57] The Public Body confirms that they do not use the automatically collected IP addresses and related information to contact individuals. The Public Body states that:

> Regarding automatically collected information, there is no effort made by the Cannabis Management Corporation to collect specific personal information of customers through IP addresses. Due to rigorous promotional / inducement restrictions embedded within the legislative framework related to cannabis sales, the Cannabis Management Corporation does not do any external push marketing that would require personal information such as a residential mailing blitz, advertising on external websites, targeted demographic/socio-economic status etc.

[58] I find that the Public Body uses the automatically collected IP addresses for the purpose for which the information was collected, which is authorized under clause 36(1)(a) of the *FOIPP Act*.

[59] The Public Body contemplates disclosing automatically collected IP addresses to a law enforcement agency, only for the purpose of a law enforcement matter. Such disclosure is permitted pursuant to clause 37(1)(o) of the *FOIPP Act*.

Date of birth to access the website

[60] To obtain access to the Public Body's website, an individual must enter their date of birth. I have already found that an individual's age is their personal information. Here, the date of birth is associated with the IP address of the user. The date of birth is also associated with an identifiable individual if they place an online order and provide identifying personal information. In either instance, whether the individual places an order, or is just browsing, the date of birth is associated with an identifiable individual and is their personal information.

[61] The Public Body's privacy policy states:

> Visiting the Website
> When visiting the Website and asked to enter your date of birth to confirm that you are 19 years of age or older to legally access the website's content, your date of birth is not used for other purposes or kept or stored by PEI Cannabis after you close your browser session.

[62] The Public Body uses the date of birth information to permit individuals access to the remainder of the website. I find that the Public Body collects the date of birth information. This finding is consistent with IR-16-001, *supra*, at paragraph 22, where it was determined that even where a public body does not retain personal information, they may still collect it.

[63] One of the purposes of the federal *Cannabis Act*, SC 2018, c. 16, enumerated at subsection 7(b), is to protect public health and safety, including protecting young persons from inducements to use cannabis. The purpose of requiring the date of birth is to ensure that those who obtain entry to the website are more than 19 years old. Some provincial cannabis online sales websites collect dates of birth, and others ask the individual to click on a check box confirming that they are over the age of 19.

[64] I am not persuaded that the date of birth is necessary for the Public Body's operations, pursuant to subsection 31(c) of the *FOIPP Act,* as there is a less invasive alternative: individuals could simply confirm that they are over the age of 19. Therefore, I find the collection of date of birth information to access the Public Body's website is not authorized under section 31 of the *FOIPP Act*.

Placing an online order

[65] In the online retail model, the Public Body collects a customer's name, address, phone number and email address, together with the details of the product and quantity of their order. I find that this is a collection of personal information. During the "checkout" process, the following message appears on the Public Body's website:

> Personal information and transactional data associated with your purchase from peicannabiscorp.com is collected, used and disclosed in accordance with the *Freedom of Information and Protection of Privacy Act* in order to process, verify and deliver your order, support product quality assurance, provide customer care, complete returns and protect against fraud. Should you have any questions regarding the collection, use or disclosure of your personal information, please contact the PEI Cannabis FOIPP Coordinator …
>
> You may also view the PEI Cannabis Privacy Policy and Terms and Conditions for further details.

[66] The Public Body contracts with two third parties to process and deliver online sales orders: Shopify, a company that processes online sales, and Purolator, a company which delivers orders. When an individual orders a product online, they are redirected from the Public Body's website to Shopify. In addition to the information about the product and quantity, the individual provides their name, address, phone number, and email address to Shopify.

[67] With respect to payment information, Shopify redirects the individual to a payment processing service to permit an individual to purchase with a debit or credit card. Neither Shopify nor the Public Body retain any personal information related to the individual's banking or credit information except that they are placing the order, the payment has been approved, and the last 4 digits of the account.

[68] When payment is confirmed, Shopify provides the order information and the personal information related to the individual to the Public Body to process the order. The Public Body sends the customer a shipping confirmation which must be presented on delivery. The Public Body discloses delivery and phone number information to Purolator to carry out delivery.

[69] The Public Body directed the Commissioner to the privacy policy on the website of Shopify. The Public Body advises the Commissioner that they intend to add the following message to their website:

> I have reviewed the Shopify Privacy Policy . . . about the collection, use and disclosure of my information, the storage and security of my information, the steps taken to protect my information, and my right to review and correct my information. I understand how the Shopify Privacy Policy applies to me.

[70] I find that collection of this personal information is authorized pursuant to subsection 31(c) of the *FOIPP Act*, as it is necessary to permit the Public Body to communicate with their customers and is directly related to the Public Body's online sales activities. I accept that the Public Body uses this personal information to process the order, and deliver it to the individual, which are the same purposes for which the information is collected. I find that these uses are authorized under clause 36(1)(a) of the *FOIPP Act*. Further, I find that disclosure of the personal information for delivery purposes is also for the same purpose for which the information was collected, and is authorized under clause 37(1)(b) of the *FOIPP Act*.

Identification at delivery

[71] When Purolator delivers the product, the delivery person may require the recipient to produce identification to confirm that the recipient is over 19 years of age. Similar to the retail setting, the delivery person inspects the identification for the purposes of confirming the individual is at least 19 years of age. They may record that they confirmed the recipient's age, but they do not record any information from the identification. I find that collecting this personal information is directly related to and necessary to confirm that individuals purchasing cannabis are over the age of 19, and that the Public Body's collection of this personal information is authorized under subsection 31(c) of the *FOIPP Act*.

[72] As this personal information is used to determine whether to leave the parcel at its destination, the use is consistent with the original purpose of collection, which is permitted under subsection 36(1)(a) of the *FOIPP Act*. As the Public Body does not record any personal information from the inspection of identification by Purolator, they are not in a position to disclose personal information.

Signature at delivery

[73] At the time of delivery, Purolator collects signatures of the recipients to acknowledge receipt of the parcel. I find that a signature is personal information of the person who provides it. The delivery service makes this information available to the Public Body to inspect online in the event that there is any dispute about whether a delivery was made.

[74] The signature of the recipient is information that relates directly to and is necessary for the Public Body's operating program of selling cannabis online. I find that the Public Body is authorized to collect the signature information pursuant to subsection 31(c) of the *FOIPP Act*, and that clause 36(1)(a) of the *FOIPP Act* authorizes the Public Body to use the signatures to confirm delivery. As the Public Body does not disclose the signature, I make no finding relating to disclosure.

Issue 4: Reasonable security arrangements

[75] Customers of the Public Body expect the privacy of their personal information to be protected, which requires reasonable security measures. Section 35 of the *FOIPP Act* states that public bodies shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, disposal or destruction.

[76] The security arrangements made by the Public Body to protect individuals' personal information are a primary concern of the Public Body, as they should be. Concerns of cannabis customers were described in a 2018 Deloitte report which studied various issues which legalization of cannabis may bring. The report, entitled *A society in transition, an industry ready to bloom - 2018 cannabis report*, stated, at page 3:

> **Customers demand privacy, security when purchasing**
> Approximately one-third of recreational cannabis consumers indicate an interest in buying products online through approved retailers' websites, and they worry about the privacy and security of their personal information. Even in-store consumers will be sharing personal information with retailers, such as allowing their ID to be scanned at point-of-sale terminals and their image captured on security cameras. The fact that governments are involved in cannabis retail means that consumers expect their information to be protected, especially online. Online retailers will need to ensure they embed privacy-by-design principles and invest in robust e-commerce cybersecurity measures.

[77] Communication with customers, and transparency of information practices, is key to addressing customers' well-founded concerns, as is ongoing attention to cybersecurity risks. These privacy issues were also outlined in the Deloitte report, *supra*, at page 27, as follows:

Online channels will need to safeguard privacy and security
Cannabis retailers' online channels will be an important source for consumers to research and discover products. While many will buy from physical locations, a substantial number of people will choose to buy online for the simple reason of privacy. Many won't want to run the risk of being seen buying cannabis while doing so still has a trace of stigma about it.

This desire for privacy extends to online sales. Consumers want to be able to trust that their personal and financial information, from login credentials to credit card numbers, are kept very secure—and very private. Online retailers will need to be painstakingly clear about what data they collect and why, and how that data will be stored, used, and shared. Cannabis consumers are especially leery of having their data shared or sold in such a way that they end up being characterized as a drug user, an unfair description for a person consuming a legal, if controlled, substance.

Consumers are also concerned about the potential for cybersecurity breaches. Given that hardly a week goes by without yet another report of such a breach, this worry is completely understandable. Cybersecurity risk is constantly evolving, and companies all along the cannabis supply chain will need to regularly update their data management and cybersecurity programs to ensure both client privacy and corporate data protection. [underline emphasis added]

Transparency of Information Practices

[78] With regard to transparency of information practices, the Public Body has been clear about what personal information they collect, and for what purpose it is used or disclosed. The Public Body is also fairly transparent about their personal information collection, including video surveillance, which is announced via signage. Their transparency will be further improved once they are compliant with the notification requirements of subsection 32(2) of the *FOIPP Act.*

[79] In the online environment, the Public Body's privacy policy is detailed and easy to understand. Initially, the Public Body's privacy policy was only available after an individual had entered their age. The Public Body plans to amend their website to permit an individual to review the terms and conditions and their privacy policy before entering the rest of the website. As the Public Body has not yet done so, I will add this to my recommendations below.

Security of Personal Information

Retail Stores

[80] The Public Body has implemented various measures to reduce the risk to personal information in their custody or control. A key part of such measures is employee training. Staff are made aware that customers' information is confidential and the breach of such confidentiality "could result in disciplinary action up to and including termination". The privacy of customer information is embedded in employees' job responsibilities.

[81] The security of video surveillance footage is also protected by the Public Body. There is a limited time frame during which the Public Body has custody or control of the footage, as the footage is over-written if there are no reported incidents. The Public Body also takes measures to limit access to the video surveillance. Video footage is stored in a locked compartment, password protected, and accessible only to a limited number of staff who are made aware of their confidentiality obligations.

[82] With respect to cameras of other customers in the retail store, the Public Body has a no-camera policy. Signage is posted, and staff are instructed to enforce the policy, and inform patrons if they are observed with a cell phone or camera. The Public Body's efforts to ensure customers' personal information is not collected by their fellow customers is a reasonable security measure which the Public Body has put in place to protect customers' personal information.

[83] The Public Body has also implemented retention and disposition schedules to ensure that, when customer information is no longer necessary to retain, it is disposed of. For example, there is a one year retention period for information relating to product returns, and the customer acknowledges this by signature.

[84] I conclude that the above-described security measures put in place by the Public Body to protect the personal information in their custody or control are reasonable. However, as with cybersecurity discussed below, the Public Body's security arrangements are found to be reasonable only at this point in time. As challenges arise, it is incumbent on the Public Body to implement the security arrangements which are reasonable at that time. In addition, continuing employee education and training is necessary to retain the culture of privacy protection at the Public Body's retail stores which currently exists. I recommend that management continue to provide regular education and training to employees relating to protection of the personal information in their custody or control.

Cybersecurity

[85] The risk of cybersecurity breaches is a growing concern for government data. This risk is further heightened where public bodies hold citizens' personal information.

[86] A factor which may increase the cybersecurity risk of the Public Body is that, before and since legalization of cannabis, organized crime has been involved in the sale of cannabis. The Information and Privacy Commissioner of British Columbia investigated a breach relating to an online casino gaming platform in Investigation Report F11-01, *Re: Investigation into a Privacy Breach of Customers' Personal Information by the British Columbia Lottery Corporation*, 2011 BCIPC 6 (CanLII). As discussed in that Report, at paragraph 31, such individuals or organizations have the means and the inclination to test the security of online platforms.

[87] Cybersecurity breaches are not limited to organized crime or other bad actors; many breaches are inadvertent. There have been privacy breaches involving cannabis

deliveries in Ontario, where Canada Post's website permitted the use of their tracking tool to obtain postal codes and the names or initials of individuals who accepted delivery of cannabis. The Public Body requires robust security measures in order to avoid such privacy breaches.

[88] In Report FI-11-01, *supra*, the B.C. Information and Privacy Commissioner, in her discussion of online risks, noted:

> [33] It is important to remember that the online environment is one of constant change. As a result, public bodies must respond quickly to any identified privacy and security risks. Failure to do so will be considered unreasonable. However, reasonableness goes beyond simply responding to identified risks. Public bodies must be proactive and implement ongoing monitoring and testing of the security of their online platforms. Public bodies must also ensure their policies are up to date and that their staff receives regular training.

[89] The British Columbia Commissioner also remarked on the diligence required in relation to the additional security risks of an online gaming platform.

> [34] While "reasonable" does not mean perfect within the context of s. 30 of FIPPA, "reasonable" does require a high level of diligence where a public body chooses to do business in the online world. Given the additional security risks of an online gaming platform, a very high level of rigour is necessary when considering the reasonableness of such security measures. The OIPC has applied this standard in our review and evaluation of BCLC's actions in response to the privacy breach.

[90] Similarly, I have applied a standard of reasonableness, taking into account the risks of online purchasing of cannabis. I find, based on the information provided to me, that the Public Body currently has reasonable safeguards in place to protect the security of personal information in their custody and control.

[91] Despite the Public Body's safeguards, I recognize that the risks of online privacy breaches, including malware, are in continuous evolution. The security of online platforms will diminish over time if development stagnates. I therefore recommend that the Public Body incorporate proactive measures into their safeguards, including periodic and comprehensive reviews and testing of their online security measures, taking into consideration known and developing online risks.

IV. SUMMARY OF FINDINGS

[92] I find that Public Body is authorized to collect and use video surveillance information for loss prevention and security, and to disclose video surveillance information for the purpose of law enforcement.

[93] I find that the Public Body is authorized to inspect an individual's identification for the purpose of confirming an individual is at least 19 years of age, during in-person purchases and during delivery of online purchases. I also find that the Public Body is authorized to use the personal information to permit entry to their retail stores, to permit customers to make purchases, and to permit customers to take delivery of online purchases.

[94] I find that the Public Body is authorized to collect and use personal information for the purpose of incident reports, inquiries and complaints, and product returns. For incident reports and product returns, I find that the Public Body is authorized to disclose personal information for law enforcement purposes.

[95] I find that the Public Body is authorized to collect and use credit and debit card information of customers at the point of sale, for the purpose of processing payment.

[96] I find that the Public Body is authorized to collect and use IP addresses of individuals for the purpose of law enforcement and web analytics. The Public Body is authorized to disclose IP addresses for law enforcement purposes.

[97] I find the collection of date of birth information to access the Public Body's website is not authorized under section 31 of the *FOIPP Act*.

[98] I find that the Public Body is authorized to collect, use and disclose a customer's name, address, phone number, email address, and the particulars of their product purchase, for the purpose of online order processing and delivery.

[99] I find that the Public Body is authorized to collect online customers' signatures at time of delivery, pursuant to subsection 31(c) of the *FOIPP Act*, and that clause 36(1)(a) of the *FOIPP Act* authorizes the Public Body to use the signatures to confirm delivery.

[100] I find that the Public Body has made reasonable security arrangements to protect the personal information in their custody or control against such risks as unauthorized access, collection, use, disclosure, disposal or destruction, in accordance with section 35 the *FOIPP Act*.

V. RECOMMENDATIONS

[101] With regard to video surveillance in the retail setting, I recommend that the head of the Public Body amend their signage to comply with the requirements of subsection 32(2) of the *FOIPP Act*, in one of the following two ways:

- indicate that video surveillance is occurring, the purpose for the collection of this personal information, the legal authority for the collection, and the title, business address and business telephone

number of an employee of the public body who can answer the individual's questions about the collection; or

- indicate that video surveillance is occurring, and direct the public to the Public Body's website policy on surveillance, which sets out the information required to satisfy subsection 32(2) of the *FOIPP Act*.

[102] I recommend that, rather than collect individuals' dates of birth in order to permit access to the Public Body's website, the Public Body should use a less invasive alternative. For example, the individual could simply confirm that they are over the age of 19.

[103] I recommend that the head of the Public Body amend their website to permit individuals to review the terms and conditions and their privacy policy before gaining access to the remainder of the website

[104] I recommend that the head of the Public Body continue to provide regular education and training to employees relating to protection of the personal information in their custody or control.

[105] I recommend that the head of the Public Body incorporate proactive security measures into their safeguards, including periodic and comprehensive reviews and testing of their online security measures, taking into consideration known and developing online risks.

[106] I thank the head of the Public Body for their ready cooperation with this investigation.

_____

Karen A. Rose
Information and Privacy Commissioner