Manitoba Ombudsman

REPORT UNDER

THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

CASE 2019-0561

MANITOBA LIQUOR AND LOTTERIES

PRIVACY IMPACT ASSESSMENT: CONTROLLED ENTRANCE INITIATIVE

SUMMARY OF COMMENT ISSUED ON SEPTEMBER 15, 2020

SUMMARY: In November of 2019 Manitoba Liquor and Lotteries (MBLL) implemented its Controlled Entrance Initiative (the initiative) with the aim of improving the safety and security of Liquor Mart stores. As a public body under the Freedom of Information and Protection of Privacy Act (FIPPA or the act), MBLL is required to comply with the privacy and access to information provisions set out in FIPPA. Our office initiated a review to assess and comment on the privacy implications of the initiative and whether the collection, use, disclosure and security of personal information of customers by MBLL complied with FIPPA. Throughout our review, MBLL worked with our office to strengthen its processes and ensure that the procedures associated with the initiative are FIPPA compliant. Our office concluded that MBLL's Controlled Entrance Initiative has complied with the requirements of FIPPA. This report highlights the importance of completing a privacy impact assessment to assess and manage the impacts of a program or initiative on individual privacy, and to ensure compliance with privacy protection rules and responsibilities under FIPPA and PHIA. While this action is not legally required in Manitoba, it assists public body or trustees to anticipate and prevent risks to personal and personal health information. Our office commended MBLL for its due diligence in completing a privacy impact assessment for the Liquor Mart Controlled Entrance Initiative and for working with our office and implementing the suggested modifications to its practices and procedures.

BACKGROUND

Throughout 2019, Manitoba Liquor and Lotteries (MBLL) considered initiatives to enhance security in Liquor Mart retail outlets in response to an increase in Liquor Mart thefts. The MBLL Controlled Entrance Initiative (the initiative) was implemented in November of 2019 with the aim of preventing thieves from entering Liquor Mart stores. The plan is to eventually equip all Winnipeg Liquor Marts with controlled entrances. At stores with controlled entrances, customers are required to present proof of age and all customers have their identification (ID) scanned and verified prior to gaining entry to a Liquor Mart.

In December of 2019, Manitoba Ombudsman began to receive questions from the public about MBLL's authority to collect personal information in connection with the initiative. Individuals who contacted our office questioned the need for MBLL to scan rather than just visually inspect ID. The public wondered about MBLL's authority to keep a scanned electronic record of their personal information. They also had questions about the amount of personal information being kept, given that ID cards may contain more information than what was required to establish age and identity. Members of the public also told our office that they did not have enough information about what would happen with their scanned personal information. As MBLL had plans to implement the initiative at all Liquor Mart retail outlets in Winnipeg, our office recognized that this project would ultimately impact many Manitobans.

As a public body under the Freedom of Information and Protection of Privacy Act (FIPPA or the act), MBLL is required to comply with the privacy and access to information provisions set out in FIPPA. In response to the concerns expressed by the public, our office initiated a review of the initiative under the following section of FIPPA:

> ***General powers and duties***
> ***49*** *In addition to the Ombudsman's powers and duties under Part 5 respecting complaints, the Ombudsman may*
> *(d) comment on the implications for access to information or for protection of privacy of proposed legislative schemes or programs of public bodies;*

The purpose of our review was to assess and comment on the protection of privacy in the context of this program and to ensure that the collection, use and disclosure of personal information is compliant with FIPPA.

On receiving notice of our review, MBLL advised our office that it was already in the process of assessing the privacy implications of the initiative using the Privacy Impact Assessment (PIA)

Tool[1] developed by our office. Subsequently, MBLL provided our office with its Controlled Entrance Initiative PIA and related documentation.

Our office reviewed the PIA and provided our comment on the privacy implications of the initiative to MBLL. We considered whether MBLL had taken steps to anticipate, identify and reasonably address privacy implications in order to ensure that their new program complies with the requirements of FIPPA and, if appropriate, the Personal Health Information Act (PHIA). Amendments to the PIA were submitted to our office as our work was ongoing. Our review reflected all information provided to us by MBLL concerning the initiative as well as our own research. This report contains an overview of the comment our office provided to MBLL.

The purpose of completing a PIA is to assess and manage the impacts of a program or initiative on individual privacy, and to ensure compliance with privacy protection rules and responsibilities under FIPPA and PHIA. Manitoba's FIPPA and PHIA do not impose any requirements for PIAs to be completed, even when new initiatives are being considered or undertaken that have significant implications for the privacy of citizens' sensitive personal or personal health information, including identification cards. Although PIAs are not mandatory in Manitoba, our office considers completion of a PIA to be a responsible practice that assists a public body to anticipate and prevent risks to personal and personal health information entrusted to it. Privacy should not be an afterthought, bolted onto a new initiative. Privacy should be considered and integrated in the planning phase so it can be embedded in the design and delivery of public services to citizens.

CONTROLLED ENTRANCE INITIATIVE SUMMARY

MBLL explained to our office that for some time it has been standard procedure that customers appearing under 25 years of age have been asked to show identification to confirm proof of age for the purchase of liquor. Under the initiative all customers will now have their ID scanned and verified prior to entering a Liquor Mart. The plan was to equip all Winnipeg and selected rural Liquor Marts with ID scanning capability by the 1st quarter of the 2020-2021 fiscal year.

As stated in the PIA, the **purposes, goals and objectives of this initiative** are:

- deterrence to crime (by deterring would-be thieves from entering Liquor Marts);
- verification of legal age to purchase liquor; and
- authentication of ID.

[1] The Manitoba Ombudsman Privacy Impact Assessment Tool is available online at https://www.ombudsman.mb.ca/info/privacy-impact-assessment.html.

In describing the scope of the Controlled Entrance Initiative, MBLL stated that security officers stationed at Liquor Mart entrances obtain valid photo identification[2] from customers and use the dedicated Patronscan system to scan, authenticate and verify the validity of the presented ID and capture limited personal information. Once an individual's ID is validated, the security officer will unlock the door to the Liquor Mart and allow entry. If the ID is not validated (expired, underage, fake, or flagged for another reason), the security officer informs the individual that they will not be permitted to enter the Liquor Mart.

Although photo identification may contain a large quantity of personal information,[3] MBLL has advised our office that its Liquor Mart Patronscan scanners use software to extract and collect only three pieces of personal information from customer ID: full name, birthdate and photo. If an individual is involved in an incident, their scanned photo will be matched against surveillance video to enable an identification. In these circumstances, the scanned personal information will be extracted from the Patronscan system and added to an internal MBLL application which is used in the management of security investigations. All other personal information collected as part of this program will be actively deleted via a prescribed database job that automatically deletes any record over 24 hours old. Access to retained personal information connected with incidents is restricted to staff with responsibility for liaising with the Winnipeg Police Services (WPS) on criminal investigations. MBLL also explained that the retained personal information may be disclosed to the WPS for investigative purposes.

COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

Collection

As noted above, MBLL collects three pieces of information about an identifiable individual, this is personal information as defined by FIPPA. No collection of personal information may take place unless authorized under FIPPA:

> ***Purpose of collection of information***
>
> ***36(1)*** *No personal information may be collected by or for a public body unless*
>
> *(a) collection of the information is authorized by or under an enactment of Manitoba or of Canada;*

[2] Valid photo identification currently accepted as proof of age include:
•Driver's licence issued in Manitoba or another jurisdiction
•Enhanced driver's licence issued in Manitoba or another jurisdiction
•Manitoba Identification Card
•Manitoba Enhanced Identification Card
•Secure Certificate of Indian Status
•Passport
Alternatively, two forms of government-issued identification may be shown, one of which must be photo ID. For more information, see 'Photo ID FAQs' on MBLL's Stop Theft web page at https://www.mbll.ca/stoptheft.

[3] For example, a Manitoba driver's licence also includes an address and signature as well as information about hair and eye colour, gender and license classification.

(b) the information relates directly to and is necessary for an existing service, program or activity of the public body; or
(c) the information is collected for law enforcement purposes or crime prevention.

MBLL has explained to our office that it is relying on clause 36(1)(c) as its authority for the collection of the personal information of Liquor Mart patrons for law enforcement purposes or crime prevention. As MBLL stated in its PIA, one of the main purposes of the initiative is crime prevention in that a controlled entrance will deter would-be thieves from entering Liquor Marts. Also, as explained above, the photos of individuals who do gain entry and are involved in incidents (such as a theft) will be matched against surveillance video to enable an identification and this information may be shared with the police for investigative purposes when a crime is committed. In light of this, our office agreed that MBLL has authority under clause 36(1)(c) of FIPPA to collect the personal information of patrons entering its Liquor Mart stores.

Our office also considered whether authority for collection may also be found in clause 36(1)(a) of FIPPA on the basis that the Liquor, Gaming and Cannabis Control Act places certain obligations on MBLL. These obligations relate to not selling liquor to a minor, not allowing the use of false ID in the purchase of liquor, and not allowing the purchase of liquor by a minor through the use of another person's ID. The relevant provisions are as follows:

No providing liquor to minors
62(1) *Except as permitted under this Act, a person must not give, sell or otherwise supply liquor to a minor.*

False identification
64(1) *A person must not attempt to purchase liquor or enter licensed premises by presenting identification that*
(a) has been altered or defaced to misrepresent the age or identity of the person;
(b) was not legally issued to him or her; or
(c) is otherwise forged or fraudulently made.

No providing identification to other persons
64(2) *A person must not provide his or her identification to a minor with the intent of enabling the minor to purchase liquor or enter licensed premises.*

As the collection of personal information from Liquor Mart patrons for the specific purposes of verifying age and authenticating ID is authorized by the above provisions under an enactment of Manitoba, in our view clause 36(1)(a) of FIPPA would also permit the collection of personal information. Having found that the authority for collection may be found in both clauses 36(1)(a) and (c) of FIPPA, our office did not consider whether authority may also be found in clause 36(1)(b), nor was it necessary to do so.

We note that, even when authorized, collection must be limited to only the amount of personal information necessary, as required by subsection 36(2) of FIPPA:

> ***Limit on amount of information collected***
> ***36(2)*** *A public body shall collect only as much personal information about an individual as is reasonably necessary to accomplish the purpose for which it is collected.*

Our office considered the personal information to be collected and the purposes for collection as stated in the PIA (and explained above). We noted that only three pieces of personal information (full name, birthdate and photo) are extracted from customer ID. We also noted that the full name and photo are the minimum amount of information necessary to make an identification in the event of a crime being committed. In our view the personal information currently collected has a clear and direct connection to the purposes as stated (deterrence to crime and verification of legal age to purchase liquor) and that collection is limited to the amount reasonably necessary for to accomplish the purpose of collection.

Collection Notice

Subsection 37(2) of FIPPA states that when personal information is collected directly from the individual the information is about (as is the case here), the individual must be informed of:

> (a) the purpose for which the information is collected;
> (b) the legal authority for the collection; and
> (c) the title, business address and telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

The intent is to ensure that individuals understand what personal information is collected, why it is needed, and who can answer any questions they may have about the collection. FIPPA does not specify how notice must be provided to an individual, and it can be provided verbally or in writing.

This information is commonly provided to an individual by means of a "collection notice." MBLL has provided our office with a sample of the Liquor Mart signage which, MBLL explained, is posted at Liquor Mart entrances. Our office examined the signage sample provided for our review by MBLL. The signage states that the personal information is being collected for crime prevention and law enforcement purposes and it provides the title, business address and telephone number of the officer of the public body who can answer questions about the collection. The sample signage we reviewed did not state the specific legal authority for collection (i.e. explanation of MBLL's authority under subsection 36(1) of FIPPA).
We noted that the sample store collection notice signage provided did not inform patrons that only three elements of personal information will be captured and retained through the scanning

process This information is provided in the Photo ID FAQ posted on www.mbll.ca/stoptheft. In our view, there are problems with relying on a web page to inform individuals already in the store about what information will be collected through the scanning process. Our office advised MBLL that this information (the elements of personal information collected) should be provided in a fair and complete collection notice.

Use and Disclosure

Once an authorized collection of personal information is made, other requirements of FIPPA relating to the use, disclosure, retention and destruction of personal information become relevant. The general duties of public bodies are described under section 42 of FIPPA:

> ***General duty of public bodies***
> ***42(1)*** *A public body shall not use or disclose personal information except as authorized under this Division.*
>
> ***Limit on amount of information used or disclosed***
> ***42(2)*** *Every use and disclosure by a public body of personal information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.*
>
> ***Limit on employees***
> ***42(3)*** *A public body shall limit the use of personal information in its custody or under its control to those of its employees who need to know the information to carry out the purpose for which the information was collected or received or to carry out a purpose authorized under section 43.*

MBLL explained that use or disclosure will only take place to make an identification in connection with the investigation of an incident. MBLL has also explained that any use will be limited to members of the Corporate Security Department as required for incident investigations.

Under clause 43(a) a public body may use personal information only for the purpose for which the information was collected or compiled under subsection 36(1) or for a use consistent with that purpose. MBLL did explain that, with regard to the use of personal information, it complies with clause 43(a) of FIPPA in that the personal information of Liquor Mart patrons will only be used for the purposes for which it is collected. MBLL also states that it complies with FIPPA's restrictions on the disclosure of personal information in that it will only make disclosures as authorized under clause 44(1)(r) of FIPPA (for law enforcement purposes or crime prevention).

Our office notes that different categories of personal information have varying degrees of sensitivity and risks associated with disclosure. Identifying the categories of personal

information collected[4] will highlight all intended uses and potential disclosures and assist in determining the level of risk in the event of a privacy breach.

ACCESS RIGHTS FOR INDIVIDUALS

One of the purposes of FIPPA is to allow individuals a right of access to records containing personal information about themselves in the custody or under the control of public bodies, (subject to the limited and specific exceptions set out in FIPPA). FIPPA also places requirements on public bodies with regard to the accuracy of personal information and the right to request a correction:

> ***Accuracy of personal information***
> ***38*** *If personal information about an individual will be used by a public body to make a decision that directly affects the individual, the public body shall take reasonable steps to ensure that the information is accurate and complete.*
>
> ***Right to request correction***
> ***39(1)*** *An applicant who has been given access to a record containing his or her personal information under Part 2 and who believes there is an error or omission in the information may request the head of the public body that has the information in its custody or under its control to correct the information.*

The above provisions are relevant to any personal information which may be retained as part of Patronscan's functions, including both the flagging of invalid ID or the flagging of a patron as a result of an incident. MBLL has explained that it will facilitate an access process and respond within 10 business days. Our office notes that the right to request correction requires that access be given under FIPPA.

While FIPPA does not have specific requirements for advising individuals about their right of access and correction, it is consistent with the duty to assist under section 9 of the act and it is good practice that public bodies will do so.

PRIVACY AND SECURITY

Administrative Safeguards - MBLL Policies and Standards

Administrative safeguards for the privacy and security of personal information include the internal policies, procedures and guidelines that are applicable to the Controlled Entrance Initiative. MBLL provided our office with copies of its draft documentation.

[4] A chart which can be used for listing the categories of personal information to be collected, used or disclosed is suggested in Part 3 of our office's PIA Tool (a sample chart is provided in the PIA Guidelines).

Our office reviewed the draft policy "Identification Requirements" and noted that the purpose of this policy as stated in the document is:

> *This policy outlines the identification requirements for access to age-restricted areas of Manitoba Liquor & Lotteries, and for purchasing liquor or lottery products.*

The statements contained in the policy are consistent with the purpose of the policy as described above and in line with the provisions of the Liquor, Gaming and Cannabis Control Act regarding the sale of restricted products to minors and the requirement to present valid ID.

Our office also reviewed the Draft Standards – Retail Stores "Liquor Mart Identification Verification." We noted that it contains standards for compliance with FIPPA on the part of security personnel, such as the requirement to sign a confidentiality agreement and undergo privacy training, as well as the use, retention and disclosure of the personal information of Liquor Mart patrons by MBLL.

Our office notes that MBLL also maintains a page titled "Privacy Policy" on its website. The information on this page consists of a "privacy notice" and a restatement of the Principles of Fair Information Practices from the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy. This web page contains the following statement:

> *Manitoba Liquor & Lotteries' Privacy & Protection of Personal Information Policy and Information Classification and Handling Procedures are in place to ensure the security and protection of all information collected, used, disclosed, stored, or destroyed, while under its control and responsibility.*

Further to our review of the Controlled Entrance Initiative PIA, we asked MBLL to provide our office with a copy of its internal "Privacy & Protection of Personal Information Policy." This general MBLL policy confirms its commitment to protecting the privacy of personal information and compliance with FIPPA. This policy specifically commits to limiting collection, use, disclosure and retention of personal information to that which is necessary for the identified business service and to obtaining consent before personal information is used for a new purpose other than that which was originally intended.

Administrative Safeguards – Contracts and Agreements

MBLL explained to our office that it has comprehensive requirements for the protection of personal information by contractors such as Patronscan, including:

> *The Contractor must:*

(i) limit access to and use of the personal information to those who need to know the information to carry out the obligations of the Contractor under the Contract;
(ii) ensure that every use of and access to the personal information by the Contractor is limited to the minimum amount necessary to carry out the obligations of the Contractor under the Contract;
(iii) ensure that each officer, staff member, agent or subcontractor of the Contractor who has access to the personal information is aware of and complies with the requirements, obligations and fair information practices in this Schedule; and
(iv) ensure that officers, staff, agents, and subcontractors who have access to the personal information sign a pledge of confidentiality, satisfactory in form and content to MBLL, that includes an acknowledgement that he or she is bound by the requirements, obligations and fair information practices in this Schedule and by the Contractor's security policies and procedures and is aware of the consequences of breaching any of them.

Technical Safeguards

Technical safeguards for the personal information of Liquor Mart patrons are described in several sections of the PIA. Our office notes that Patronscan's website states that all its data centers are SSAE16 SOC 2 certified, security reviewed facilities with industry standard server and security technology.

The PIA also states that all MBLL Patronscan users will have a role-based access profile and password and their access to personal information will be logged. Additionally, Patronscan employees who have access to MBLL customer data as part of their technical support role will have an individual profile and password and their access will also be logged. The PIA states that the system has full audit functionality and MBLL will monitor who accesses and/or retrieves patron ID information for law enforcement purposes on a quarterly basis. Our office also notes that a section of the Draft Standards – Retail Stores "Liquor Mart Identification Verification" state that information related to access will be auditable and can be retrieved at any time.

Records Management

MBLL explained that most personal information collected as part of this program will be actively deleted via a prescribed database job that automatically deletes any record over 24 hours old.[5] As explained earlier, the scanned personal information related to incidents and investigations will be extracted from the Patronscan system and added to an internal MBLL application which is used in the management of security investigations.

[5] MBLL has provided information which explains that any 'live data' - personal information collected from driver's license scans - older than 23 hours is deleted on an hourly basis.

MBLL has also explained that SQL[6] server back-ups of scanned data are performed daily and the backup is retained until overwritten, a maximum of 48 hours. The purpose of SQL back-up files is to restore a corrupted database and the information is not readable outside of the database structure.

MBLL stated that all of its corporate records are scheduled and that retention requirements for the records associated with the Controlled Entrance Initiative will be documented in its contract with Patronscan.

The PIA explained that paper records are limited to a "vestibule security checklist" used to provide daily counts of the reasons for refusing entry (e.g., minor, intoxicated, disorderly). These will be housed by store managers. Similar statistics (regarding reasons for refusal) will also be maintained by Patronscan. MBLL advised that these statistics are aggregate and do not contain personal information.

Information Manager

Under FIPPA, a public body must enter into an information manager agreement if it discloses information to an information manager outside the public body. FIPPA sets out the requirements for information managers (such as Patronscan) under section 44.1. The PIA indicated that, as part of contracting agreements, MBLL requires vendors to sign Schedule B: Protection of Personal information and Schedule C: IT Security Safeguards and Measures. MBLL also explained that its contract with Patronscan outlines Patronscan's security measures, MBLL's privacy obligations and Patronscan's use of personal information.

Our office noted that MBLL's schedules B and C contain specific and detailed requirements for the protection of personal information in compliance with the requirements of FIPPA. Schedule B requires that contractor employees who have access to personal information complete training on the protections required by MBLL and complete a pledge of confidentiality. Schedule C contains requirements that must be met regarding technical security (such as the encryption of confidential information in transit), secure destruction, notification in the event of a privacy breach and provisions concerning the audit of compliance with MBLL's requirements (as set out in the schedules). Our office noted that MBLL requires that all records of confidential information must be destroyed in a manner that makes it impossible to read or reconstruct the information.

CONCLUSIONS

Based on our review of MBLL's PIA and other information related to the Controlled Entrance Initiative, our office concluded that MBLL was authorized to collect the personal information of

[6] SQL stands for Structured Query Language. SQL facilitates access to and manipulation of databases.

patrons as part of its initiative and that this collection was limited as required under FIPPA. We provided comments to strengthen notice to individuals about the collection to ensure people are fully informed of the specific personal information being collected. Our office also concluded that MBLL has made reasonable security arrangements to safeguard personal information and to prevent unauthorized access, use, disclosure and destruction. MBLL has also complied with the requirements of FIPPA concerning the retention of personal information and has implemented records schedules to ensure the secure destruction of personal information which is no longer required to be retained.

In the course of our review of the PIA, our office identified areas of privacy risk which were identified to MBLL. MBLL has since taken steps to address the privacy risks identified by our office.

MBLL should be commended for its due diligence in completing a PIA for the Liquor Mart Controlled Entrance Initiative and for the modifications that have already been made to its practices and procedures in response to feedback from our office.

Manitoba Ombudsman
September 15, 2020