RETAIL COUNCIL OF CANADA

GUIDING PRINCIPLES ON PRIVACY FOR RETAILERS IN CANADA

BROUGHT TO YOU BY

Retail Council of Canada

PROTECTING INFORMATION, AND YOUR BRAND

BROUGHT TO YOU BY STEPHEN O'KEEFE AND RETAIL COUNCIL OF CANADA

IN 2001, an Act was created to protect Canadians from inadequate and irresponsible handling of their personal information. Prior to this, there were a number of incidents where criminals assumed the identity of individuals whose personal information was compromised through some form of nefarious act or simple negligence.

The "Personal Information and Protection of Electronics Documents Act" (PIPEDA), was established to address this issue. The Act includes language that guides businesses concerning ways they should treat personal information obtained from customers they have business dealings with.

As it relates to retail loss prevention, The Act inadvertently created hurdles to overcome in the fight to combat retail crime. Examples of this are as follows; prior to the Act, (1) retailers collaborated and shared information related to known criminals and suspicious actors, including their personal information, (2) frequent refunders of merchandise were listed in log books for the purpose of monitoring their shopping patterns to identify and mitigate against the risk of abusive and fraudulent refunds.

After the implementation of PIPEDA, several practices were abandoned, including information sharing amongst investigators of different organizations and the listing of customer names in log books. The result: criminals took advantage and were able to become anonymous. The log books were destroyed by retailers in the wake of several consumer complaints that the lists were not compliant with the new Act. Additionally, retailers abandoned the practice of sharing information as advised by their respective independent legal advisors. The Act did recognize the need to share information between investigative bodies, resulting in an exemption for these groups. However, the same classification did not include mainstream retailers.

In March 2017, changes were made to the Act following a submission (Bill S4) that received Royal Assent in June 2015. Bill S4 covered a number of aspects related to breaches, but also contained language relative to the sharing of information between organizations. These changes were specific to the sharing of information related to criminal activity. Retail Council of Canada (RCC) also reviewed some of the complaints that were previously related to refund activity and determined that the operational practices in 2003 were a breach of the Act, however in a very limited and specific area of PIPEDA.

The purpose of this paper is to clarify, (a) the guiding principles of PIPEDA and the practical applications associated with them, (b) the guidelines related to the sharing of information between organizations specifically related to the investigation of a contravention of a law in Canada, and, (c) the guidelines associated with the request for identification from a customer for the purpose of completing a refund transaction.

RCC stresses that these are guidelines and recommendations of operating practices and in no way suggest that this document be used for the purpose of providing a legal opinion to its members. The association recommends that independent legal opinions be obtained to advise each independent company.

Stephen O'Keefe
External Consultant
Retail Council of Canada

O'Keefe has been working within the discipline of loss prevention for more than 30 years, protecting numerous brands, including Hudson's Bay Company, Walmart and others. He's been awarded for his contributions to the retail industry and loss prevention sector, and is recognized by his peers as an expert within these fields.

THE GUIDING PRINCIPLES

PRINCIPLE #1

ACCOUNTABILITY

Guidance:

The bottom line? Assign an owner and create a plan. Compliance to PIPEDA is critical for several reasons. But, most importantly, to protect the personal information of customers, as well as to avoid being subject to an investigation by the Office of the Privacy Commissioner of Canada.

It is recommended that over and above assigning one owner that businesses develop a "Privacy Committee" made up of key individuals from areas such as HR, Legal, Risk Management and Loss Prevention. This will ensure that the legal aspects are addressed, that the people component is covered, and that the inspection and audit requirements are incorporated into a plan.

"An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles."

PRINCIPLE #2

IDENTIFYING PURPOSES

Guidance:

This requires written policies and procedures, as well as training guidelines. The key aspect to this area of PIPEDA is that the purpose is clearly articulated and that the organization also treats the personal information with the intended purpose; that they limit use for the purpose clearly understood by the individual whose information is collected.

In the case of a refund transaction, if you intend to use a form of identification for the purpose of protecting your organization against fraud, it is recommended that you clearly state the purpose. And if you use software to encrypt and create a unique identifier, explain this process to your customer upon requesting a form of identification.

"The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected."

PRINCIPLE #3

CONSENT

Guidance:

Consent can be obtained in two ways; explicit or implied consent. An example of implied consent is when an organization prominently states to customers that they use CCTV to protect the premises. Given the ubiquitous nature of security cameras, if a customer proceeds to shop in your store, it's assumed you have received implied consent to collect their personal information, which in this case would be their video image.

"The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."

PRINCIPLE #4

LIMITING COLLECTION

Guidance:

Keep it simple. Collect only the bare minimum of information for your organization to meet its business needs. Any extra information might place you in harm's way. And the reality is, it is an unnecessary burden and expense for you to secure such extra personal information collected.

"The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means."

PRINCIPLE #5

LIMITING USE, DISCLOSURE, AND RETENTION

Guidance:

The bottom line is that once you have collected personal information, and intend to use it for purposes other than the originally agreed upon terms with your customer, you essentially have to start over with the identifying purpose and consent stages. If there is a term for the length of time, say one (1) month, your organization should have a strict process whereby the personal information is appropriately destroyed on the day following the end of the month.

"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes."

PRINCIPLE #6

ACCURACY

Guidance:

If you collect it, you are accountable for it, and it should be as accurate as if it was your own personal information. In most cases this can be satisfied if you (1) get your customer to complete the information personally, or (2) ask your customer to verify that the informati2on that you have collected is complete and accurate.

"Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."

PRINCIPLE #7

SAFEGUARDS

Guidance:

Much like the requirement to protect credit card information, retailers need to ensure the proper CCTV coverage is considered, as well as access control to restricted areas where "data" is stored—in this case personal information.

"Personal information shall be protected by security safeguards appropriate to the sensitivity of the information."

PRINCIPLE #8

OPENNESS

Guidance:

Referring back to the aspect of ownership, all employees must be able to refer a customer to the provisions set forth in their policies and procedures as it relates to your Privacy Policy. In the event that this cannot be located, the owner can be consulted quite easily IF this is planned on the frontside and communication internally is appropriate.

"An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."

PRINCIPLE #9

INDIVIDUAL ACCESS

Guidance:

This particular principle is one that requires considerable thought and very clear language directing the organization internally. Consider this; as an organization, you have collected information about an individual. Let's use the Loss Prevention department as an example. That individual then asked to view the "file", and in amongst the valid documents there lies some other information that you were unaware of because others have placed details of the individual's personal information in it. Think of the issues this raises: consent was not obtained, the collection was not lim-

"Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."

ited to the purpose identified...a whole host of issues come to light.

A best practice in this area is to vet the connection of information. Always view the collection in terms of "what if the individual walked in today and asked what was being collected, and demanded to see the information immediately". This is a good litmus test, and will likely keep you out of harm's way.

PRINCIPLE #10

CHALLENGING COMPLIANCE

Guidance:

There should be two (2) ways to challenge an organization. Many businesses fail to implement a first course, and therefore the only other option is the second—notifying the Office of the Privacy Commissioner of Canada who will likely launch an investigation. The first course of action should be a way for the individual to report through to the "owner" of the Privacy Policy. They should then assume the role of lead investigator and launch a formal internal investigation. Keep in mind that if you select your internal legal counsel for this role, and if you expect that this will provide you with "solicitor/client privilege" as a way to protect the findings, you may be okay.

"An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance."

Sharing without consent:

Privacy requirements are in place to protect all parties interested in the collection of personal information. And the law has the unintended consequence at times of providing some form of anonymity to the criminals. In March 2017, the Act was amended to allow for organizations to share information in limited fashion, without the consent of an individual. Specifically, it states that:

"7(3) ...an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is;

(d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;

(d.2) made to another organization and is reasonable for the purposes of detecting or suppressing fraud or of preventing fraud that is likely to be committed and it is reasonable to expect that the disclosure with the knowledge or consent of the individual would compromise the ability to prevent, detect or suppress the fraud"

Guidance:

RCC has been advocating for these changes on behalf of members. The changes allow for retailer "x" to inform retailer "y" of a criminal act that is about to be perpetrated against them without having to ask the criminal for permission to share that information.

Be Forewarned:

The Act also details specific requirements that an organization must meet concerning ways to handle that sharing of such personal information;

"Even though information-sharing may occur in specified circumstances without consent, an organization is still required to fulfill its other PIPEDA obligations, including but not limited to, limiting the disclosure of personal information, safeguarding it, and ensuring that any disclosure of personal information is only for purposes that a reasonable person would consider are appropriate in the circumstances."

Guidance:

This, in essence, means that with the exception of consent, all other areas of the guiding principles must be respected.

The Office of the Privacy Commissioner of Canada (OPCC) is a Federal body. Provinces have a Provincial version and corresponding legislation which may or may not be consistent with the Federal Office. It is recommended that organizations review both Federal and Provincial statutes to ensure they take into consideration any of the innuendos which may affect their policies and procedures.

For further information please contact;

Stephen O'Keefe
External Consultant
Retail Council of Canada
sokeefe@retailcouncil.org
905-821-4651

Further reference material from the Office of the Privacy Commissioner of Canada can be accessed at:
www.priv.gc.ca/media/2038/guide_org_e.pdf