OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

Order P05-01

K.E. GOSTLIN ENTERPRISES LIMITED

David Loukidelis, Information and Privacy Commissioner
May 25, 2005

Quicklaw Cite: [2005] B.C.I.P.C.D. No. 18
Document URL: http://www.oipc.bc.ca/orders/OrderP05-01.pdf
Office URL: http://www.oipc.bc.ca
ISSN 1198-6182

Summary: The organization operates a Canadian Tire store. When returning goods to the store, the complainant declined to provide her name, address and telephone number. The organization's notices of purpose of collection comply with PIPA, although the organization is encouraged to improve them. PIPA permits the organization to require individuals to provide this personal information and to use it as part of its efforts to detect and deter fraudulent returns of goods. This information is "necessary" for that purpose under s. 7(2). The organization cannot, however, require individuals to provide such personal information for the purpose of customer satisfaction follow-up, a purpose and use that must be made optional for customers. Section 35(2) does not authorize the organization to retain personal information permanently, but no retention period is suggested.

Key Words: personal information—reasonable person—appropriate in the circumstances—necessary—retention of personal information.

Statutes Considered: B.C.: *Personal Information Protection Act*, ss. 2, 7(2), 10, 11 & 35(2); *Personal Information Protection Regulations*, s. 6. **Canada**: *Personal Information Protection and Electronic Documents Act*, ss. 3, 5(3), Schedule 1 (principles 4.3.3 and 4.4). **Quebec**: *An Act Respecting the Protection of Personal Information in the Private Sector*, articles 5(1) and 9; *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*.

Authorities Considered: Order 01-52, [2001] B.C.I.P.C.D. No. 55; Order No. 12-1994, [1994] B.C.I.P.C.D. No. 12; Order 00-07, [2000] B.C.I.P.C.D. No. 7.

Cases Considered: *R. v. Clark*, 2005 SCC 2, [2005] S.C.J. No. 4; *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, [2004] F.C.J. No. 1043; *Englander v. Telus Communications Inc.*, 2004 FC 387, [2004] F.C.J. No. 1935; *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, [2004] S.C.J. No. 44; *Air BC Ltd. v. C.A.W.-Canada, Local 2213* (1997), 61 L.A.C. (4th) 406; *NorthwesTel Inc. and I.B.E.W., Loc. 1574, Re* (1996), 55 L.A.C. (4th) 57; *G., Re*, (1984), 51 Nfld. & P.E.I.R. 263 (Nfld. U.F.C.); *X. c. Allôstop*,

C.A.I. 941538, March 1995; *X. c. Résidence L'Oasis Fort-Saint-Louis*, [1995] C.A.I. 367; *X. c. Synergic International, 1991 Inc.*, [1995] C.A.I. 361; *La Personnelle vie, Corporation d'Assurance c. Cour du Québec*, [1997] C.A.I. 466 (S.C.); *Bellerose c. Université de Montréal*, [1992] C.A.I. 240 (C.Q.); *Bayle c. Université de Laval*, [I992] C.A.I. 240 (C.Q.); *A. c. C.*, [2003] C.A.I. 534; *Société de transport de la Ville de Laval c. X.*, [2003] J.Q. No. 1284, [2003] C.A.I. 664 (C.Q.); *Mélanie Julien c. Domaine Laudance (Beaudet et Saucier Inc.)*, [2003] C.A.I. 77; *Société de transport*, [2003] J.Q. No. 1284, [2003] C.A.I. 664 (C.Q.); *R. v. Oakes*, [1986] 1. S.C.R. 103; *Comeau c. Bell Mobilité*, [2002] C.A.I. 1 (discontinuance of the motion to authorize appeal (C.Q., 2002-05-14)); *Moses c. Caisse populaire Notre-Dame-de-la-Garde*, [2002] C.A.I. 4.

1.0 INTRODUCTION

[1] The issue in this case is whether the *Personal Information Protection Act* ("PIPA") permits a retailer to require someone who is returning goods to provide identifying personal information for the purpose of combatting fraudulent returns of goods.

[2] The organization involved, K.E. Gostlin Enterprises Limited ("organization"), is an Ontario corporation that is extra-provincially registered in British Columbia. It has operated the Canadian Tire Store in Kelowna since 1981 and does so under a franchise agreement with Canadian Tire Corporation, Limited ("CTC").

[3] On June 22, 2004, the complainant, a customer, went to the store to return an item she had purchased a few days before. She provided the customer service clerk with the item's sales receipt and the Canadian Tire money related to the purchase. According to the complainant, the clerk asked for her name, telephone number and birth date.

[4] The complainant declined to provide any personal information to the clerk. A discussion ensued and the store's customer service manager became involved. She told the complainant that, if she refused to provide her personal information, the store could refuse any refund because of the need to protect against fraud. The complainant asked to see a copy of the organization's privacy policy. It could not be located right away and the employees told the complainant that they would find a copy and provide it to her later. When the complainant continued to resist providing her personal information, the store processed the refund anyway. The complainant was told, however, that the store might, in future, refuse to process refunds without the requested personal information.

[5] That same day, the complainant wrote to the store to complain, expressing concern that the requirement for personal information violated privacy legislation and seeking a response. The store's general manager responded on July 13, 2002, assuring the complainant that her personal information "is not sold, shared or released to any party unless required by law" and that the information

> …is required for the protection of our business and more importantly, our customers. Controlling losses ensures the store's ability to serve its customers' needs at competitive prices. Having such information will also allow follow up in the event there has been an error in the return's processing by the store.

[6] The customer complained to this Office and, mediation under s. 49 of PIPA having failed, the matter was referred to a written inquiry under Part 11 of PIPA.

[7] I invited and received representations from CTC, the Canadian Tire Dealers' Association ("CTDA"), the Retail Council of Canada ("RCC") and the BC Civil Liberties Association ("BCCLA"). I am grateful to each organization, although I have, of course, decided this matter based only on the evidence and law applicable to the complaint at hand.

2.0 ISSUES

[8] The notice of inquiry issued says the issue is whether "the practice and the published policy of the organization to collect personal information from customers returning merchandise" comply with ss. 7, 11 and 35 of PIPA.

3.0 DISCUSSION

[9] **3.1 Appropriateness of *In Camera* Evidence and Argument**—Some of the organization's evidence and argument were submitted on an *in camera*, or confidential, basis. The BCCLA says that its ability to argue its position has "been impaired" by the fact that it did not see the *in camera* material.

[10] Section 50(2) of PIPA, like s. 56(2) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), provides that an inquiry "may be conducted in private". Section 50(4) of PIPA reads as follows:

> (4) The commissioner may decide…
>
> (b) whether a person is entitled to be present during, to have access to or to comment on representations made to the commissioner by another person.

[11] This provides authority for verbal or written proceedings that are in whole or in part *in camera*.

[12] Further, like ss. 47(1) and (3) of FIPPA, ss. 41(1) and (3) of PIPA restrict the information that the commissioner may disclose in conducting an inquiry such as this.

[13] In an early FIPPA decision, Commissioner David Flaherty decided that s. 56(4)(b) of FIPPA, which is worded almost identically to s. 50(4)(b) of PIPA, provides authority to accept *in camera* "affidavits in written hearings that may not, in whole or in part, be disclosed to another party (or intervener, if any)".[1] In arriving at this conclusion, he also noted the prohibition in s. 47(3)(b) in FIPPA against disclosure of certain information. Noting the similarities between FIPPA's and PIPA's provisions on this issue, I am satisfied that similar authority exists in an inquiry under Part 11 of PIPA.

[14] In this case, I have concluded, it is appropriate to hold *in camera* the commercial information that the organization has submitted on that basis.

[1] Order No. 12-1994, [1994] B.C.I.P.C.D. No. 12. Also see Order 00-07, [2000] B.C.I.P.C.D. No. 7.

[15] **3.2 The Context: Fraudulent Returns of Stolen Goods**—The organization relies on two affidavits sworn by its president, Keith Gostlin. He deposed in his February 16, 2005 affidavit ("Gostlin Affidavit No. 1") that the Kelowna Canadian Tire store processes more than 70,000 merchandise refund transactions each year; almost 200 returns are processed on an average day (paras. 15 & 29, Gostlin Affidavit No. 1). The value of merchandise returned each year is a significant percentage of the store's gross revenues. More important, although I cannot reveal the actual amount or percentage of revenues, which have been appropriately submitted *in camera*, the organization's annual losses due to fraudulent merchandise returns are material and significant (Gostlin Affidavit No. 1). The organization has implemented a number of security measures to prevent theft and fraud, ranging from in-store video surveillance to careful checking of employee references on hiring (para. 8, Gostlin Affidavit No. 1).

[16] Keith Gostlin's evidence speaks to how a material percentage of profits is lost each year to theft and fraud. He gives details about the various methods people use to defraud the organization through the return of stolen goods. These activities are possible because the organization, as a Canadian Tire operator, has, like many other large (but not necessarily small) retailers, a policy of permitting returns (para. 13, Gostlin Affidavit No. 1). The organization has adopted this policy even though, Keith Gostlin says, the law does not generally require a retailer to undo a sale and offer a refund (para. 12, Gostlin Affidavit No. 1).

[17] Barbara Nilsen, the organization's customer service manager, is in charge of refund processing. In her February 16, 2005 affidavit ("Nilsen Affidavit"), she deposed that stolen merchandise is returned to the store for fraudulent refunds on "an ongoing basis" (para. 3). One of the duties of customer service desk staff is to "try to limit the number of fraudulent return transactions" by applying the store's return policy (para. 3, Nilsen Affidavit).

[18] Despite the organization's various loss-reduction measures, it still incurs losses from merchandise theft and from fraud and attempted fraud in the return of goods stolen from the organization's store or from Canadian Tire stores elsewhere in the region (paras. 9 and 10, Gostlin Affidavit No. 1). These losses are made worse by the fact that, when the organization refunds money, the refund includes the item's purchase price plus a further 14%, to reflect the British Columbia social services tax and federal goods and services tax ostensibly paid on the goods.

[19] The broader picture, according to the CTDA, is that theft and fraudulent merchandise returns are not unique to the Kelowna Canadian Tire store, since "a serious problem with theft and fraudulent merchandise returns also exists, to a greater or lesser degree, at every Canadian Tire Associate Store across Canada" (para. 9, CTDA submission). The CDTA says "theft of merchandise which is subsequently returned for fraudulent cash refunds has become a sophisticated illegal 'business' operation which results in significant losses to our member Associate Dealers" (para. 11). It refers to examples from Ontario in which police detected sophisticated theft and fraud-related activities involving Canadian Tire stores (paras. 12 and 13).

[20] The RCC has more than 9,000 members across Canada in the retail sector. Its members include national retail chains, independent stores and other retailers. The RCC

has periodically studied losses to retailers from theft, fraud and other activities. Its 2003 Canadian Retail Security Report indicated that "the total retail sales lost due to theft were over $3 billion annually or $8 million each day" (p. 3, RCC submission). The largest part of these losses stems from theft, but the RCC says these figures are relevant because stolen products are often returned fraudulently for refund (p. 3). The RCC describes the attractions of fraudulent merchandise returns for criminals this way (p. 3):

> One area where our members report a rapid growth of criminal activity is at the returns desk. Retailers' generous returns policies have attracted criminals who have seen a low risk, high-reward way to make money. A stolen article can be moved through a fence for perhaps ten cents on the dollar. Only certain easily resold types of merchandise can be fenced and retailers have taken many steps to protect this merchandise. The beauty of returns fraud is that any stolen article of any value can be returned for 115 percent of its value (price plus taxes). Thus a stolen and returned jug of windshield washer fluid may bring a criminal more money than the theft and fencing of a power tool.

[21] Echoing Keith Gostlin's evidence, the RCC says that most retailers have flexible refund and exchange policies to "provide good customer service and customer satisfaction" (p. 4). Faced with what the RCC says is "a rapid increase in returns fraud", the RCC adds (at pp. 5 & 6), retailers

> …have had to improve their procedures regarding returns while maintaining good customer service. This of necessity has required better information about returns and the individuals who make them.

[22] This information is used by many retailers, the RCC indicates, to analyze the risk that a particular return of goods may be fraudulent. At p. 6, the RCC says retailers have identified a number of "strong indicators that a transaction may be an attempt to get money from a retailer fraudulently", including these:

- Frequent returns by the same customer;
- Multiple refunds made to different individuals at the same address;
- Returns of product unaccompanied by a receipt;
- An unusually high level of returns without receipt (may be a sign of employee collusion;)
- Above-average returns of the same product (also useful as a warning of product performance and quality problems;)
- A volume of returns that is excessive in relation to the volume sold;
- Returns of an unusual type of product such as a product that is purchased to be used immediately (e.g. consumable products;) and
- The presentation of counterfeit receipts of credit or debit card slips along with stolen merchandise. (This is typically a gang-related activity.)

[23] Personal information is "essential", according to the RCC, to help a retailer decide whether a fraud is being attempted (p. 7). The collection of personal information also deters fraud because (p. 7):

> …criminals abhor visibility. Our members advise us that the mere request for personal information will cause some customers to refuse or leave the desk immediately. Our members recognize that some legitimate customers genuinely object to providing personal information. But it has also proven to be a strong indicator of fraud. Those retailers who ask for an address to which they can send a cheque reimbursing the customer are confident that a customer who refuses this information has a high likelihood of being a fraudster. The normal business response is simply to decline to accept a return of the product.

[24] The material before me establishes that some individuals return stolen goods to retailers using receipts that they have obtained illegitimately. In other words, the fact that someone who is returning an item produces a receipt does not mean the item was not stolen or that the receipt genuinely relates to the item being returned.

[25] To summarize, the material before me establishes that there is a real, not merely a perceived or minimal, problem with the fraudulent return of stolen goods by supposed customers, with or without sales receipts in hand. The organization has other loss prevention measures in place, but collection and use of identifying personal information is, it says, an important feature of its overall loss-reduction efforts.

[26] **3.3 The Organization's Practices & Policies**—The Canadian Tire merchandise refund policy is followed by the organization and Canadian Tire stores across Canada (para. 14, Gostlin Affidavit No. 1). The Canadian Tire policy allows customers to return merchandise within 90 days of purchase "for product exchange or cash refund with receipt" (para. 14, Gostlin Affidavit No. 1). This policy is brought to customers' attention in three ways.

[27] First, the following notice (a copy of which is Exhibit 4 of Gostlin Affidavit No. 1) is posted at each cashier station in the store:

> Easy returns: save your receipt
>
> To return an item for an exchange or refund, bring it to any Canadian Tire store within 90 days, in its original condition and packaging, with your receipt and issue of Canadian Tire 'Money'™. Valid photo ID may be required.
>
> Details at our Customer Service desk. Some exceptions may apply.

[28] Each sales receipt, a copy of which is Exhibit 5 of Gostlin Affidavit No. 1, has the following statement on its back:

> Easy Returns: Save Your Receipt
>
> To return an item for an exchange or refund, bring it to any Canadian Tire store within 90 days, in its original condition and packaging, with your receipt and issue of Canadian Tire 'Money'.
>
> Without receipt, returns will be processed at our discretion for a store credit based on the lowest selling price of the item. Valid photo ID may be required.

[29] The front of each receipt contains the following statement:

> Please retain receipt and Canadian Tire money for full refund. Valid photo ID may be required.

[30] In addition, the organization's customer privacy policy (a copy of which is Exhibit 6 of Gostlin Affidavit No. 1) says this:

> **2. We let you know why we are collecting your personal information**
>
> The store will identify the purpose for which your personal information is collected. We do this before the information is actually collected. Examples of why we collect personal information include:
>
> - Communicating with you generally or to ensure customer satisfaction, and receiving your complaints where that applies
>
> …
>
> - Processing and keeping track of sales and service transactions to serve you and for internal business use
> - Protection against fraud and error in order to protect our customers and our business
>
> …
>
> Types of information collected include:
>
> **Individual Purchases**
>
> This store ensures that it limits requests for information to what is required to ensure excellent customer service currently and in future, and in the interests of recommending products and services to you that are believed will be of interest and provide value to you. Most of the information is very basic, needed to complete a purchase; examples include name, address, telephone number, credit card or bank account information, debit card information, information printed on your personal cheques, details of identification provided if paying by cheque (to guard against fraud), and a description of the item(s) requested or purchased.
>
> **Refunds**
>
> The same information that is required to complete an individual purchase may also be required for a refund. In addition, for the protection of our business and our customers, this may also necessitate a receipt and photo identification. Controlling losses assures the store's ongoing ability to service its customers' needs at competitive prices. Having such information will also allow follow up in the event there has been an error in the return's processing by the store.
>
> …
>
> **Complaints**
>
> Personal information, particularly your name and contact number, may be requested and taken from you in order to address and resolve your concerns and complaints on merchandise purchased or the service experienced in our store. Without this information,

> we may not be able to fully investigate these, put them right to the extent possible, or advise you on the outcome.

[31] Keith Gostlin deposed that copies of the customer privacy policy are available at the customer service desk and that a notice of the policy's existence and availability is posted in the store (para. 21, Gostlin Affidavit No. 1). This notice, a copy of which is Exhibit 6 of Gostlin Affidavit No. 1, tells customers that a copy of the privacy policy is "available upon request". In his March 9, 2005 affidavit ("Gostlin Affidavit No. 2"), however, he acknowledged that, because they could not provide the complainant with a copy of the policy, store employees have been reminded about the organization's privacy compliance obligations and reminded that they must make copies of the policy available at the customer service desk on request (para. 4).

[32] According to Keith Gostlin, anyone who asks why the organization requests the name, address and telephone number of the individual, or their photo identification, is told that the information is used to prevent fraud and to contact the individual in case of any error in the refund (para. 23, Gostlin Affidavit No. 1). He also said individuals are told their personal information may be used to contact them to see if they have experienced any problems in relation to their refund (para. 23, Gostlin Affidavit No. 1). Barbara Nilsen deposed as follows:

> 33. On the few occasions where customers have asked why we require photo identification or name, address and telephone number, when I explain that we do so to prevent fraud, to be able to contact customers if an error has occurred in processing the refund, and to contact customers to determine whether they were satisfied with the refund transaction, these customers accepted my explanation and proceeded with their return transaction.

[33] The organization's evidence on the process followed in refund processing can be summarized as follows:

- Anyone who wishes to return goods to the Kelowna Canadian Tire store is directed to the customer service desk.
- The individual is asked for his or her telephone number. The telephone number is used as a file number or locator to gain access to the file associated with that number. If the individual has not returned something to the store before, he or she is asked to provide name, address and telephone number. This information is entered into the store's computer.
- Store employees enter information about the goods being returned, for inventory control, restocking and tax purposes.
- The employee records the date and place of purchase, price, internal product number, form of payment, whether a receipt has been produced, the reason for the return and whether the purchase was exempt from taxes.
- After all of this information has been entered, a return form is printed, the individual signs the form acknowledging receipt of the refund and the refund is processed.

[34] In some cases, store employees may ask for proof of identity (para. 27, Gostlin Affidavit No. 1):

> In certain circumstances we may ask for photo identification to verify the identity of the customer. Asking for photo identification operates as a significant deterrent to refund fraud. In our experience persons who seek to obtain fraudulent refunds generally try to provide as little information as possible, and are invariably reluctant to provide photo identification. Since most returns are made by local residents, normally the photo identification would be a British Columbia driver's license, British Columbia Identification Card or sometimes other photo identification such as a Costco member card. The customer service desk employee notes on the return voucher form that the customer's identity has been confirmed by photo identification, and specifies the type of photo identification shown.

[35] Keith Gostlin further deposed as follows (Gostlin Affidavit No. 1):

> 30. Once a customer's name, address and telephone number are entered into the computer system, any subsequent merchandise return transactions for that customer can be processed quickly. Since some of our customers have the same or similar names, for example "Bob Jones" or "Robert Jones" or "Rob Jones", the fastest and most accurate way to retrieve the customer's correct information, and print the required return voucher form, is to search the database for the customer's telephone number. Sometimes there may be 10 or 15 customers lined up at the customer service desk waiting to return merchandise. We must be able to provide service to our customers as quickly and efficiently as possible to maintain the customer relationship upon which the success of the business depends.
>
> 31. We rely on the ability to review a customer's own merchandise return history to reveal possible return of stolen merchandise, or a pattern of merchandise usage followed by return of the merchandise for a cash refund.… [*in camera* evidence deleted]
>
> 32. Where a customer's merchandise return history, or a return transaction reveals fraud, we are able to record that information to assist our customer service employees to identify possible future fraudulent returns. For example the telephone number provided by a customer can link back to previous fraud attempts. Some examples of return transaction histories which are used to alert customer service employees are attached collectively as Exhibit 9.
>
> 33. Obtaining a customer's name, address and telephone number permits us to be able to contact the customer if, as sometimes occurs, there has been an error in processing the return.

[36] Barbara Nilsen's affidavit added this about use of the store's computer for these activities:

> 37. Given the volume of returns we process every day, it would be virtually impossible to process these returns if we did not do so using our computer technology. It would make no sense to process returns by manually filling out the return voucher forms. Recording personal information also permits us to

> more quickly process refund transactions. When our customers return merchandise, it is evident that they want the return transaction processed quickly. We work in a very competitive industry and it is extremely important that we are able to provide the best customer service possible. The fact that we record personal information on our computer system permits us to establish a pattern of fraudulent behaviour which might not otherwise be disclosed. We are also able to contact our customers to determine if they have been satisfied with the transaction process.

[37] The organization only uses an individual's name, address and telephone number in connection with that individual's own return transactions. The personal information cannot be accessed by anyone other than Kelowna Canadian Tire store employees who work in the customer service department and store management (para. 28, Gostlin Affidavit No. 1; para. 6, Gostlin Affidavit No. 2). The information is not "disclosed to any third party except if required by the police in connection with criminal activity at the store" (para. 28, Gostlin Affidavit No. 1).

[38] **3.4 Interpreting PIPA**—As the Supreme Court of Canada affirmed earlier this year, it is now clearly established that "the words of an Act are to be read in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention" of the legislature.[2]

[39] This approach, of course, governs PIPA's interpretation, just as the Federal Court of Canada has applied it when interpreting the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), the federal private sector privacy law that is similar to PIPA.[3]

[40] Section 2 of PIPA states PIPA's "object", or purpose:

> **Purpose**
>
> 2. The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[41] This legislative purpose statement is similar, although not identical, to that found in s. 3 of PIPEDA:

> **Purpose**
>
> 3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[2] *R. v. Clark*, 2005 SCC 2, [2005] S.C.J. No. 4, para. 43.
[3] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, [2004] F.C.J. No. 1043, para. 184 (F.C.).

[42] The Federal Court of Appeal has said this about PIPEDA's purpose and its interpretation:[4]

> 38. The purpose of the PIPED Act is altogether different [from the federal public sector *Privacy Act*]. It is undoubtedly directed at the protection of an individual's privacy; but it is also directed at the collection, use and disclosure of personal information by commercial organizations. It seeks to ensure that such collection, use and disclosure are made in a manner that reconciles, to the best possible extent, an individual's privacy with the needs of the organization. There are, therefore, two competing interests within the purpose of the PIPED Act: an individual's right to privacy on the one hand, and the commercial need for access to personal information on the other. However, there is also an express recognition, by the use of the words "reasonable purpose", "appropriate" and "in the circumstances" (repeated in subsection 5(3)), that the right of privacy is not absolute.
>
> …
>
> 46. …[E]ven though Part 1 and Schedule 1 of the Act [PIPEDA] purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests….

[43] Section 2 of PIPA persuades me that these observations apply equally to PIPA's interpretation. PIPA recognizes the interest of individuals in controlling the collection, use and disclosure of their personal information, but it also acknowledges the need of organizations to collect, use and disclose personal information.

[44] **3.5 Notice of Collection**—I will deal first with questions of notice and consent under ss. 7 and 10. The notice of inquiry mentions as an issue whether the organization complied with s. 7 of PIPA, which raises the question of whether consent was given and whether the organization gave the complainant the information required under s. 10(1). Both the organization and the BCCLA argued these issues.

[45] Section 10(1) of PIPA requires an organization to give notice of the purpose for collection of personal information at or before the time the information is collected, failing which the consent is, as s. 7(1) contemplates, not valid. The relevant portions of ss. 7 and 10 read as follows:

> **Provision of consent**
>
> 7(1) An individual has not given consent under this Act to an organization unless
>
> (a) the organization has provided the individual with the information required under section 10(1), and
>
> (b) the individual's consent is provided in accordance with this Act.…
>
> …

[4] *Englander v. Telus Communications Inc.*, 2004 FC 387, [2004] F.C.J. No. 1935 (C.A.).

Required notification for collection of personal information

10(1) On or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing

(a) the purposes for the collection of the information, and

(b) on request by the individual, the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.

…

(3) This section does not apply to a collection described in section 8 (1) or (2).

[46] Notice of the purpose for collection is not required, as s. 10(3) says, where either s. 8(1) or s. 8(2) applies. Although the notice of inquiry does not mention it, the organization itself has raised s. 8(1), saying that an individual's consent to the collection of personal information is deemed to be given, as provided in s. 8(1), because the purpose for collection would be obvious to the reasonable person. As this issue is not mentioned in the notice of inquiry, I make no finding on it, although I will say in passing that the organization's arguments on s. 8(1) were not compelling on first impression.

[47] The BCCLA argues that the organization's notice of the purpose for collection of personal information is not adequate. It says the notice does not "give an adequate or even accurate description of what the policy is, which is the collection of name, home phone and address and the inputting of this information into a store computer system" (para. 13, BCCLA submission). The BCCLA argues that the notice contains a fatally vague purpose statement because it "does not clarify that the personal information is being put into a databank and is therefore too nebulous to be the basis for a proper consent" (para. 16).

[48] It is true the various notices do not specifically describe each of the precise data elements that the organization collects, but the notices do tell individuals that identifying personal information may be collected and details of the information collected are given through verbal notice when the individual returns an item. As for notice that the collected information will be kept in electronic form, the organization's employees give verbal notice to this effect at the time a refund is processed.

[49] I conclude that the organization provided notice of the purpose for its collection of personal information sufficient to satisfy PIPA. It did so through the notice of collection posted at cashier stations, the written notices on the front and back of the sales receipt, through its privacy policy and through the verbal notice that store employees gave to the complainant when the return transaction was initiated.

[50] Although I have found that the notice is adequate, I have done so with some hesitation in these relatively early days of PIPA's existence. The organization's statement, through the various avenues described above, that identifying information is collected "to prevent fraud" should be clarified. The organization should consider clarifying the printed notices found on sales receipts and at cashier stations. The notices should ideally say something to the effect that the collected information is used to help the organization ensure that returns by particular individuals are valid in each case and over time. The notices that state "valid photo ID may

be required" could be amended, for example, to say "identifying information will be required for returns and valid photo ID may also be required". The various forms of printed notice should also more clearly notify customers of the collection of personal information for customer satisfaction follow-up and managing errors in refunds.

[51] **3.6 Are the Organization's Purposes for Collection Appropriate?**—The next question is whether the organization's practice and policy comply with s. 11, which reads as follow:

> **Limitations on collection of personal information**
>
> 11 Subject to this Act, an organization may collect personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> (a) fulfill the purposes that the organization discloses under section 10 (1), or
>
> (b) are otherwise permitted under this Act.

[52] Would a "reasonable person" consider that the purposes for which the organization collects this personal information are "appropriate in the circumstances"?

[53] I do not agree that, as the BCCLA argues, the appropriate test for s. 11 of PIPA is the test articulated by the Privacy Commissioner of Canada in Case Summary 114 (January 23, 2003),[5] a test that was later largely adopted by the Federal Court in the same case[6]. Case Summary 114 contains the following passage:

> The Commissioner acknowledged that the company's stated purposes, namely, to reduce vandalism and theft, improve staff security, and limit the potential liability for damages, would seem to be appropriate. However, to ensure compliance with the intent of section 5(3), the Commissioner stressed that the circumstances must also be considered. In determining whether the company's use of the digital video cameras was reasonable in this case, he found it useful to consider the following questions:
>
> - Is the measure demonstrably necessary to meet a specific need?
> - Is it likely to be effective in meeting that need?
> - Is the loss of privacy proportional to the benefit gained?
> - Is there a less privacy-invasive way of achieving the same end?

[54] Case Summary 114 dealt with an employer's video surveillance of employees without employee consent. Without foreclosing the possibility that some or all of these questions perhaps might be of some assistance in other kinds of cases under PIPA, I do not find them useful here.

[55] Section 11 of PIPA invokes the standard of "a reasonable person". This is an objective standard—the idiosyncrasies, likes, dislikes or preferences of a particular individual

[5] PIPEDA case summaries are available through www.privcom.gc.ca.
[6] *Eastmond* v. *Canadian Pacific Railway*, above, note 3.

do not determine the outcome. As s. 2 affirms, PIPA aims to balance the "right" of individuals to protect their personal information and the "need" of organizations to collect, use and disclose personal information. Under s. 11, one has to decide whether the hypothetical reasonable person, knowing the purposes for collection and the surrounding "circumstances", would consider the purposes for collection to be "appropriate". Relevant circumstances may include the kind and amount of personal information being collected, the uses to which it will be put and any disclosures the organization intends at the time of collection.

[56] Turning to the situation here, what "circumstances" surround the organization's policy on return of goods? The organization collects and uses identifying personal information from individuals who seek to return goods for, primarily, the purpose of identifying and deterring fraud.[7] As indicated earlier, the fraudulent return of goods is a significant and widespread problem, one that directly affects the organization. A number of the roughly 70,000 return transactions the organization processes each year are attempted or successful frauds. Like other retail organizations in Canada, the organization loses profits each year to theft and fraud, including returns fraud. It is appropriate to infer that, if losses mount, they may have an impact on the prices consumers pay for goods—retailers can be expected to pass on the cost of fraud in the form of higher prices for goods wherever possible. A reasonable person would know this and would take it into account.

[57] Another consideration is the kind and amount of personal information involved here. The organization collects the name, address and telephone number of an individual who is returning goods. It may ask the individual to confirm identity with photo identification, but the evidence indicates the organization does not collect the particulars of the identification used.[8]

[58] It is also relevant that an individual's name, address and telephone number cannot in and of themselves generally be considered sensitive information. This kind of information is available in telephone directories except where an individual's name and address are unlisted. Section 6 of the *Personal Information Protection Act Regulations* provides that "the name, address, telephone number and other personal information of a subscriber that appears in a telephone directory or is available through directory assistance" is "publicly available" information and, by virtue of s. 12(1)(e), s. 15(1)(e) and s. 18(1)(e), respectively, PIPA dispenses with an individual's consent to collection, use or disclosure of this information so long as the directory or directory assistance service is available to the public and the subscriber can refuse to be included. These provisions do not apply in this case, of course, but they underscore the fact that an individual's name, address and telephone number are generally speaking of a non-sensitive nature.

[59] Here we have a retail organization facing ongoing challenges from attempted and successful fraudulent returns of goods, with the organization suffering losses each year due to fraudulent return of stolen goods. We also have collection and use of identifying information that is generally publicly available and non-sensitive in nature. That information is collected

[7] The organization may also use the personal information to do a customer satisfaction follow-up with the customer. I return to this issue below.
[8] I address this issue below as well.

and used to detect and deter fraudulent returns of goods as part of its overall loss-reduction strategy. The evidence also shows that the organization does not disclose the personal information to anyone else, except to the police for fraud or theft investigations resulting from the organization calling the police.

[60] In light of these circumstances, I conclude that a reasonable person would consider the organization's fraud and loss prevention purpose for collecting and using identifying personal information to be "appropriate in the circumstances". I reach the same conclusion regarding the customer satisfaction and refund error management purposes for collection.

[61] **3.7 Is the Personal Information "Necessary"?**—Section 7(2) recognizes that an organization can require someone to provide personal information, as a condition of doing business, but only where the personal information is "necessary" to provide the product or service:

> **Provision of consent**
>
> …
>
> (2) An organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.

[62] The question, then, is whether the organization can require someone who wishes to return goods to provide her or his name, address and telephone number as a "condition of supplying a product or service", on the basis that the information is "necessary" to provide the product or service.

Supply of a product or service

[63] No one argues in this inquiry that a refund transaction does not involve the supply of a product or service. British Columbia law does not as a general matter require a seller of goods to unwind the sales contract if the goods are not defective or unfit for their intended purpose. The complainant in this case returned the goods because she decided they were not the right colour for her purposes, but her right to return them did not arise out of consumer protection legislation, sale of goods law or some other exception to the usual rule that sales transactions are final. Her right to do so stemmed from the organization's agreement, as a term of the sales contract, to unwind the sale and refund the price if the complainant met certain conditions. Those terms of sale—which included the terms on which the sale would be unwound—suffice in my view to fit this situation within s. 7(2). The refund, which reversed the product's supply, was part of its supply.

What does "necessary" mean in s. 7(2)?

[64] An organization's ability to require consent to collection of personal information relies, again, on whether the personal information is "necessary to provide the product or service." What did the Legislature intend the word "necessary" to mean in s. 7(2)?

[65] This word's meaning varies depending on the context in which it is used, as the Supreme Court of Canada acknowledged last year in a case dealing with s. 2.4(1)(b) of the *Copyright Act*. Binnie J. said this for the majority:

> The words of s. 2.4(1)(b) must be read in their ordinary and grammatical sense in the proper context. "Necessary" is a word whose meaning varies somewhat with the context. The word, according to *Black's Law Dictionary*,
>
> > …may mean something which in the accomplishment of a given object cannot be dispensed with, or it may mean something reasonably useful and proper, and of greater or lesser benefit or convenience, and its force and meaning must be determined with relation to the particular object sought. [Emphasis added… [by Binnie J.]]
>
> (*Black's Law Dictionary* (6th ed. 1990), at p. 1029)[9].

[66] The following more complete quote from the *Black's Law Dictionary* (6th ed.) definition emphasizes this:

> This word must be considered in the connection in which it is used, as it is a word susceptible of various meanings. It may import absolute physical necessity or inevitability, or it may import that which is only convenient, useful, appropriate, suitable, proper, or conducive to the end sought. It is an adjective expressing degrees, and may express mere convenience or that which is indispensable or an absolute physical necessity. It may mean something which in the accomplishment of a given object cannot be dispensed with, or it may mean something reasonably useful and proper, and of greater or lesser benefit or convenience, and its force and meaning must be determined with relation to the particular object sought.[10]

[67] So, the word "necessary" is not destined to mean "indispensable". Its meaning depends on the context in which it is found.

Decisions under similar Canadian laws

[68] Quebec's public and private sector privacy rules restrict collection and use of personal information in certain ways, and do so by applying the concept of necessity. Article 9 of Quebec's 1994 private sector privacy law ("Quebec Law")[11] imposes restrictions similar to those in s. 7(2) of PIPA. Article 9 reads as follows:

> **Goods and services**
>
> **9.** No person may refuse to respond to a request for goods or services or to a request relating to employment by reason of the applicant's refusal to disclose personal information except where

---

[9] *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, [2004] S.C.J. No. 44.

[10] *Air BC Ltd. v. C.A.W.-Canada, Local 2213* (1997), 61 L.A.C. (4th) 406 (McPhillips), p. 423, quoting from *Black's Law Dictionary* (6th ed.) at p. 1029. Also see, to similar effect, *NorthwesTel Inc. and I.B.E.W., Loc. 1574, Re* (1996), 55 L.A.C. (4th) 57 (S. Kelleher Q.C.), p. 73, and *G., Re*, (1984), 51 Nfld. & P.E.I.R. 263 (Nfld. U.F.C.), p. 267.

[11] *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., c. P-39.1.

1) collection of that information is necessary for the conclusion or performance of a contract;

2) collection of that information is authorized by law; or

3) there are reasonable grounds to believe that the request is not lawful.

Doubt

In case of doubt, personal information is deemed to be non-necessary. [12]

[69] Article 5 of the Quebec Law also limits collection to that which is "necessary":

Necessary information

5. Any person collecting personal information to establish a file on another person or to record personal information in such a file may collect only the information necessary for the object of the file.

[70] Article 64 of Quebec's public sector access to information and privacy law[13] limits public body collection of personal information:

Unnecessary information.

64. No person may, on behalf of a public body, collect nominative information if it is not necessary for the carrying out of the attributions of the body or the implementation of a program under its management.

[71] The Commission d'accès à l'information du Québec ("CAI") enforces both the Quebec Law and Quebec's public sector access and privacy law. Some CAI decisions under the Quebec Law have held that "necessary" means "indispensable". For example, in *X. c. Allôstop*[14] the issue was whether an organization could, under article 5, require as a condition of membership renewal that a member provide her or his social insurance number. Reference was made to a statutory interpretation text to support the view that "necessary" refers to that which is absolutely indispensable. The social insurance number was held not to be indispensable for the purpose of renewing a membership.

[72] In another 1995 decision, *X. c. Résidence L'Oasis Fort-Saint-Louis*,[15] the CAI held that an employer could not require job applicants to provide their social insurance numbers, bank name, bank account numbers and certain other personal information as a condition of considering their job applications. This information was not "necessary", within the meaning of article 9(1) of the Quebec Law, at the job application stage.[16]

---

[12] English versions of all quoted Quebec statutes are provided on-line by the Éditeur officiel du Québec: http://www.publicationsduquebec.gouv.qc.ca.

[13] *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, R.S.Q. c. A-2.1.

[14] C.A.I. 941538, March 1995.

[15] [1995] C.A.I. 367.

[16] Also see *X. c. Synergic International1991 Inc.*, [1995] C.A.I. 361.

[73] While these and other decisions—including a number under Quebec's access and privacy law[17]—appear to have embraced the stricter test of indispensability, others have approached the matter by looking at the relevant factual context and the purpose for collection in deciding what is necessary.[18]

[74] More recently under the Quebec Law, in *A. c. C.*,[19] Commissioners Stoddart, Constant and Grenier dealt with a case in which a landlord had required a prospective sub-lessee of a house to provide fairly extensive personal information, including information about the tenant's employment, a blank cheque, a T4 slip, her banking details and a consent to a credit check. The Commissioners said that the question of whether personal information is "necessary" for the purposes of articles 5 and 9 of the Quebec Law depends on the circumstances of each case. They quoted with approval the following passage from the Court of Quebec's decision in *Société de transport de la Ville de Laval c. X.*:

> …It is not a question of determining what necessity is in itself so much as deciding, in the context of the protection of personal information, and for each case, what is necessary for the accomplishment of each particular purpose...[20]

[75] Before saying this, the Court in *Société de transport* had cautioned against interpreting "necessary" too strictly or too liberally" and added this:

> …[It is] unproductive to tie oneself to a fixed definition of necessity and to a technical application of that one criterion, without considering the particular facts of each case, the type and the nature of the information in issue and the objectives pursued by the organization. Accordingly, the interpretation should permit a more dynamic criterion, one that is more accurate and also better suited to evaluation of the merits of each case.[21]

[76] Filion J. expressed the view that such an interpretive approach serves both the letter and spirit of the law.[22] He then went on to develop a new test for determining what personal information is "necessary", a test based on that in *R. v. Oakes*,[23] which dealt with

---

[17] It has been held that interpretations of Quebec's public sector law also apply to the Quebec Law. See *La Personnelle vie, Corporation d'Assurance c. Cour du Québec*, [1997] C.A.I. 466 (S.C.).

[18] The contextual approach is reflected in, for example, *Bellerose c. Université de Montréal*, [1992] C.AI. 240 (C.Q.); *Bayle c. Université de Laval*, [I992] C.A.I. 240 (C.Q.). For a discussion of this issue, see R. Doray & F. Charrette, *Accès à l'information: Loi annotée, jurisprudence et commentaires* (Éd. Yvon Blais: Cowansville, 2001), at p. III/64-3.

[19] [2003] C.A.I. 534.

[20] [2003] J.Q. No. 1284, [2003] C.A.I. 664 (C.Q.), para. 33 (Filion J.). My translation. The same three Commissioners of the CAI took a similar approach, again in the housing rental context, in *Mélanie Julien c. Domaine Laudance (Beaudet et Saucier Inc.)*, [2003] C.A.I. 77.

[21] *Société de transport*, above, at para. 30. My translation.

[22] *Société de transport*, above, at para. 33. *Société de transport* involved Quebec's public sector access and privacy law. As in earlier court decisions, the Court in *Société de transport* expressed the view that the interpretation of "necessary" in Quebec's public sector law is relevant to its interpretation under the Quebec Law.

[23] [1986] 1 S.C.R. 103. The test applied in Case Summary 114, discussed above in relation to s. 11 of PIPA, also appears to draw heavily on the *Oakes* test, which dealt with state action and not private sector conduct. As I indicated earlier, without foreclosing the possibility that some or all of the questions stated in the Case Summary 114 test might be of some assistance in other kinds of cases under PIPA, I do not find them useful in relation to s. 7(2), the language of which also differs from s. 1 of the *Charter*.

constitutionality of legislation or state action under the *Canadian Charter of Rights and Freedoms.*

[77] As for PIPA, the Legislature did not, in my view, intend the word "necessary" in s. 7(2) to mean "indispensable". PIPA's legislative purposes[24], the overall statutory context in which the word "necessary" appears and the language of s. 7(2) lead me to conclude that the Legislature did not intend to create a strict standard of indispensability by using the word "necessary".

[78] Personal information may be "necessary" under s. 7(2) even if it is not indispensable. Of course, personal information may, in some cases, be "necessary" in the sense that it is not possible to supply a product or service without the personal information or because it is legally required for the supply.[25] But there will be cases where personal information is "necessary" even though it is not, when considered in a searching yet reasonable manner, indispensable in the sense that it is not possible to supply the product or service without the personal information.

[79] Recognizing the differences in legislative language between PIPEDA and PIPA, I find support for this view in decisions under PIPEDA. Principle 4.3.3 of Schedule 1 to PIPEDA has a purpose similar to that of s. 7(2) of PIPA, although Principle 4.3.3 uses the word "required" and not "necessary":

> **4.3.3**
>
> An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate, purposes.

[80] Schedule 1 of PIPEDA also uses the criterion of necessity:

> **4.4 Principle 4—Limiting Collection**
>
> 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.

[81] Several PIPEDA cases have involved the issue of whether a telephone or cell phone service provider can require a would-be subscriber to provide identification to open an account. For example, Case Summary 94 (December 2, 2002)[26] involved a service provider's

---

[24] Article 1 of the Quebec Law says its purpose is to establish rules for organizations that collect, use and communicate personal information in the course of carrying on an enterprise. It expressly incorporates into the Quebec Law the privacy rights found in articles 35 to 40 of the *Civil Code of Quebec*. There is in article 1 no balancing of the interests and needs of organizations that is found in s. 2 of PIPA.

[25] As an example of legal necessity, under British Columbia law, it is "necessary" in a house sale for the lawyer or notary to collect the name and address of both seller and buyer in order to complete the sale and properly register the transaction in the land title registry.

[26] Other PIPEDA decisions that deal in similar ways with requirements to provide identifying personal information include Case Summary 202 (August 5, 2003), Case Summary 204 (August 5, 2003), Case Summary 217 (August 5, 2003), Case Summary 256 (October 1, 2003) and Case Summary 288 (February 1, 2005).

requirement that would-be subscribers provide identifying personal information before the organization would supply services. The organization said the information was needed to do a credit check in order to establish credit-worthiness. The then Privacy Commissioner upheld the requirement, finding that it violated neither principle 4.3.3 of Schedule 1 nor s. 5(3) of PIPEDA, which is similar in intent and language to s. 11 of PIPA, since a reasonable person would consider the purpose for collection to be appropriate in the circumstances.

[82] As regards principle 4.3.3, Case Summary 94 says this:

> The Commissioner noted that, although the collection was an acknowledged condition of the supply of service, it was not an absolute condition, in that the company as a matter of policy allowed an alternative in the form of a security deposit—an alternative the Commissioner did not deem to be unreasonable. All things considered, he found that the company was in compliance with Principle 4.3.3.

[83] There is some suggestion in this passage from the summary that the existence of an alternative to the supply of identifying information—the payment of a security deposit—was a factor in the Commissioner's finding of compliance with principle 4.3.3. I note, in any event, the fact that the case involved an organization that sought identifying information in order to protect itself against financial loss, which is what the organization here is trying to do.

[84] A similar decision is Case Summary 280 (October 26, 2004), which involved a subscription for satellite telecommunications services. An individual tried to buy satellite equipment but refused to provide photo identification and a credit card when the seller, in order to combat signal theft, required him to provide that information. The case summary suggests that the requirement for photo identification changed at some point to a requirement that the individual supply his name, address and telephone number. Assistant Privacy Commissioner Heather Black decided that "the company requires the photo ID for purposes a reasonable person would consider are appropriate in the circumstances, that is, to combat signal theft". She further decided that the "fact of requiring a credit card—or pre-authorized payment—to purchase the equipment is necessary to fulfill the explicitly specified, and legitimate purposes, that is, contribute towards combatting satellite piracy." There was no violation of principle 4.3.3 or s. 5(3) of PIPEDA. It is not clear from the summary whether principle 4.4 was directly in issue in this case. It is noteworthy, however, that Assistant Commissioner Black found that collection of identifying information was "necessary" and appropriate in order to combat signal theft, *i.e.*, to protect the financial interests of the organization and others.

[85] I acknowledge that PIPEDA's language differs somewhat from PIPA's. But these PIPEDA cases deal with legislation that has a legislative purpose similar to PIPA's and they deal with the question of what personal information is "necessary" for purposes identified by an organization. These cases suggest that, under PIPEDA, a service provider can require someone who wants to enter into a service agreement to provide identifying personal information on the basis that it is "necessary" to provide a service where a business is trying to protect itself from loss due to fraud by requiring customers to identify themselves. I see no material difference between a requirement for customer identification for loss-prevention purposes at the outset of the supply of services or goods and identification for loss-prevention

purposes when an organization and customer are unwinding a retail sale, which is the situation at hand.

[86] Again, I have found that the organization's purpose for collecting an individual's name, address and telephone number is appropriate under s. 11. I am also persuaded that this identifying information is "necessary" under s. 7(2) in order to return goods for a refund, as agreed to under the terms of sale. The organization is therefore able to require someone to provide this information as a condition of unwinding the sale and refunding the purchase price. The circumstances of each case will govern, of course. In this case, I have considered a number of factors in concluding that the personal information in question is necessary for loss prevention purposes.

[87] First, as noted earlier, this kind of personal information is generally available to the public and it is generally not sensitive in nature.

[88] The second factor has to do with the purpose for collection. This is not a case where an organization seeks to collect personal information to use it as an asset or to turn it to collateral advantage. It loses money to fraud each year and has reasonably decided to implement a risk management strategy, of which this is one component. The transaction is, as envisaged by the sale terms, limited to the sale's reversal, something the organization is only required to do because it agrees to do so, contractually, on the terms it advertises (including regarding the provision of identifying information).

[89] Third, the organization does not require an excessive amount of personal information. It limits its requirements to basic identifying information—name, address and telephone number—that is directly related to and minimally required in order to achieve the organization's legitimate purposes.

[90] For these reasons, I find that the personal information the organization requires its customers to provide in order to return goods is, considered in a searching yet reasonable manner, "necessary" for that particular transaction. This is not to suggest that an organization can impose contractual terms on an individual that attempt to contract out of PIPA's requirements in whole or in part. I have serious reservations about any suggestion that one can validly derogate from PIPA's minimum standards or protections by contract.

[91] I have reached a different conclusion about the organization's collection and use of personal information for the purpose of customer satisfaction follow-up. The organization uses an automated telephone-dialling program to call customers and give them the option of providing feedback on their experience in returning goods. I have already found that a reasonable person would consider that purpose for collection appropriate under s. 11, but compliance of this practice with s. 7(2) is a different matter. Without adopting the BCCLA's contention that the organization's automated customer satisfaction follow-up calls are "clearly a marketing tool", I find that the organization's use of personal information for customer satisfaction follow-up is not "necessary", as contemplated by s. 7(2), for the supply of the product or service in question. The organization cannot in my view require an individual to consent to provision of personal information for the purpose of customer satisfaction follow-up. It can seek consent, but not force it.

[92] The organization therefore must make it clear in the appropriate notices that an individual is not required to provide personal information for the purpose of customer satisfaction. The organization cannot refuse to proceed with a refund transaction if the individual declines to give personal information for the purpose of being contacted by telephone. I make this finding even though the organization's evidence indicates that the script of the automated follow-up call gives individuals the choice to participate or not.

[93] Two further points about confirmation of identity are desirable. As indicated above, one factor in my decision here is that the organization does not ask for an excessive amount of personal information. It limits its requirements to basic identifying information. As mentioned earlier, the complainant says that store employees asked for her date of birth, but the organization says this is not so (Nilsen Affidavit, para. 5). It is not clear to me that an individual's date of birth would be "necessary" within the meaning of s. 7(2) of PIPA. If the organization did ask for this information, my preliminary view is that it should be optional and must be clearly so.

[94] Similarly, the evidence indicates that the organization in some cases asks for photo identification to confirm identity—one can assume that a driver's licence will typically be produced—but the organization does not record personal information from the identification that is shown. Although a preliminary view, and the circumstances of each case would govern, I have some doubt that an organization is able to compulsorily collect or use personal information from identification such as a driver's licence on the basis that the information is "necessary" within the meaning of s. 7(2). I would think it is enough for the organization to examine the identification, which is what the organization does in this case, and then record the fact that it was produced and examined to the organization's satisfaction.[27]

[95] **3.9 Retention of Customer Information**—The last issue is whether the organization's apparently indefinite retention of personal information complies with s. 35 of PIPA:

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

[27] In this respect, I note that Quebec's CAI has on many occasions held that a driver's licence number, social insurance number or Quebec health insurance number can be collected and used only for the purposes for which they were created. See, for example, *Comeau c. Bell Mobilité*, [2002] C.A.I. 1 (discontinuance of the motion to authorize appeal (C.Q., 2002-05-14)); and *Moses c. Caisse populaire Notre-Dame-de-la-Garde*, [2002] C.A.I. 4.

[96] The organization says the return voucher form that is printed during the processing of a refund, and signed by the customer, is kept for roughly three months and then destroyed. It acknowledges, however, that the name, address and telephone number of an individual are retained indefinitely.

[97] The organization says this does not violate s. 35(2). It argues that, because of the volume of refunds it processes each year and the fact that it has "many repeat customers", whose ongoing business it strives to maintain, retention of this personal information is important "to both the store and its customers because this allows subsequent merchandise return transactions to be processed quickly and efficiently" (p. 12, initial submission). It argues, without supporting evidence, that if its customers cannot quickly process refunds, it "is only reasonable to expect that they will shop somewhere else where they are able to do so" (p. 12).

[98] The organization contends that indefinite retention of personal information is necessary because "refund fraud may not be discovered until revealed through a pattern of transactions", meaning its ability "to reveal a customer's return history is important in discovering possible fraud" (p. 13). It submits (p. 3, initial submission) that requiring it to destroy a customer's

> …merchandise return history after some set period of time would benefit only those "customers" who seek to defraud the store. No benefit to honest customers can be demonstrated, especially since their name, address and telephone number is not disclosed outside the store and is not used for any purpose except in connection with their own merchandise return transactions.

[99] Section 35(2) does not, as the organization suggests in this passage, require a demonstrated "benefit" to "honest customers" or anyone else. The only question is whether the organization is required to destroy personal information when it is "reasonable to assume" that the purpose for which the information was collected is no longer being served by its retention and further that retention of the information is no longer necessary "for legal or business purposes".

[100] In considering this issue, it is appropriate to take into account the nature and extent of the personal information involved, any applicable legal requirements (such as statutory limitation periods for civil lawsuits) and the business purposes relating to retention of the personal information.

[101] The personal information involved here is not, as I have already noted, generally of a sensitive nature. Its permanent retention is not, however, justified on that basis alone. While I acknowledge the personal information is useful to detect possible patterns of fraudulent activity, I am not persuaded it is reasonable to assume that this purpose will always continue to be served, such that permanent retention is permitted under s. 35(2)(a).

[102] Further, the organization has not pointed to any "legal…purposes" that, as s. 35(2)(b) contemplates, require indefinite retention. As regards "business purposes" mentioned in s. 35(2)(b), a good deal of the organization's evidence addresses other loss reduction strategies it employs and tactics its customer service employees use, exercising their judgment

and experience, in identifying potentially suspicious refund transactions. The organization has not pointed to any "business purposes" that, as s. 35(2)(b) contemplates, require indefinite retention of the personal information.

[103] I therefore find that s. 35(2) does not permit the organization to permanently retain the personal information described above. On the evidence at hand, I am not in a position, nor am I prepared, to suggest a specific retention period. The organization should, however, formulate a schedule for retention of personal information, keeping s. 35(2) in mind, and implement a retention schedule that complies with s. 35(2).

4.0 CONCLUSION

[104] For convenience, I will summarize here the main conclusions in this case:

- Like FIPPA, PIPA authorizes the commissioner to receive *in camera* evidence and argument in appropriate cases.

- Some individuals return stolen goods to retailers using receipts that they have obtained illegitimately. The fact that someone who is returning an item produces a receipt does not mean the item was not stolen or that the receipt genuinely relates to the item being returned.

- There is a real problem with the fraudulent return of stolen goods by supposed customers, with or without sales receipts in hand. The organization has other loss prevention measures in place, but collection and use of identifying personal information is, it says, an important feature of its overall loss-reduction efforts.

- The organization's notice of the purpose for collection of personal information satisfies PIPA. The printed notices should, however, be clarified. The printed notices should also more clearly notify customers of the collection of personal information for customer satisfaction follow-up and managing errors in refunds.

- The s. 11 standard of "a reasonable person" is an objective one. The idiosyncrasies, likes, dislikes or preferences of a particular individual do not determine the outcome. As s. 2 affirms, PIPA aims to balance the "right" of individuals to protect their personal information and the "need" of organizations to collect, use and disclose personal information. Under s. 11, one has to decide whether the hypothetical reasonable person, knowing the purposes for collection and the surrounding "circumstances", would consider the purposes for collection to be "appropriate". Relevant circumstances may include the kind and amount of personal information being collected, the uses to which it will be put and any disclosures the organization intends at the time of collection.

- A reasonable person would consider the organization's fraud and loss prevention purpose for collecting and using identifying personal information to be "appropriate in the circumstances", as s. 11 requires. I reach the same conclusion regarding the customer satisfaction and refund error management purposes for collection.

- Under s. 7(2) of PIPA, personal information may be "necessary" even if the information is not indispensable to the supply of the product or service in a strict, causation-like, sense or because the supply would be legally impossible without the personal information. Personal information may in some cases be "necessary" because it is indispensable to the supply of the product or service. There will, however, be cases where personal information is "necessary" even though it is not, when considered in a searching yet reasonable manner, indispensable in the sense that it is not possible to supply the product or service without the personal information. There will almost certainly be a reasonably high degree of need for the personal information, but not indispensability in the sense just given.

- Here, the required identifying information is "necessary" under s. 7(2) in order to return goods for a refund, as agreed to under the terms of sale. The organization is therefore able to require someone to provide this information as a condition of unwinding the sale and refunding the purchase price.

- By contrast, the organization's use of personal information for customer satisfaction follow-up is not "necessary" for the supply of a product or service. The organization cannot require an individual to consent to provision of personal information for that purpose—it can seek consent, but not force it. The organization must make it clear in the appropriate notices that an individual is not required to provide personal information for the purpose of customer satisfaction.

- The evidence indicates that the organization in some cases asks for photo identification to confirm identity but the organization does not record personal information from the identification. Although a preliminary view, it is doubtful that an organization could establish that collection and use of personal information in photo identification such as a driver's licence are "necessary" within the meaning of s. 7(2).

- Although the collected personal information is useful to detect possible patterns of fraudulent activity, its permanent retention is not permitted under s. 35(2). Although I suggest no specific retention period, the organization should turn its mind to the question of retention periods under s. 35(2) and decide on and implement a policy that complies with s. 35(2).

[105] In light of the above findings, under s. 52 of PIPA I make the following orders:

1. I confirm that the organization, K.E. Gostlin Enterprises Limited, is in compliance with s. 11 respecting its collection and use of personal information for the purposes, as discussed above, of fraud and loss prevention, customer satisfaction follow-up and refund error management and confirm its decision to collect and use personal information for those purposes,

2. I confirm that the organization, K.E. Gostlin Enterprises Limited, is in compliance with s. 7(2) respecting its collection and use of personal information for the purpose, as discussed above, of fraud and loss prevention and refund error management and confirm its decision to collect and use personal information for those purposes,

3. I require the organization, K.E. Gostlin Enterprises Limited, to comply with s. 7(2) respecting its collection and use of personal information for the purpose, as discussed above, of customer satisfaction follow-up by not requiring any individual, as a condition of accepting merchandise for return, to consent to the collection, use or disclosure of personal information for the purpose of customer satisfaction follow-up, and

4. I require the organization, K.E. Gostlin Enterprises Limited, to perform its duty under s. 35(2) by destroying its documents containing personal information, or removing the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that (a) the purpose for which that personal information was collected is no longer being served by retention of the personal information and (b) retention is no longer necessary for legal or business purposes. The organization is to deliver to me a retention schedule respecting personal information that it collects, uses and discloses for the purposes dealt with in this order within 60 calendar days after the date of this order, together with such supporting material or evidence as it considers desirable.

May 25, 2005

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia