New Privacy Legislation: What it means to your business

Credifax Atlantic Limited
Fall 2003 Seminar

David T.S. Fraser
David.fraser@mcinnescooper.com
(902) 424-1347

October 17, 2003

1

Focus on Canadian Privacy Law

Introduction to the
Personal Information Protection and Electronic Documents Act

2

What is Privacy?

- Has been characterised as the right to be left alone, to be secure in one's home and free from unwanted interference
- In the context of the new law, privacy means having control over one's personal information
  - Choice of whether to disclose information at all
  - Control over with whom it is shared
  - Control over how it is used
  - Don't lose control once you've released your information "into the wild"

3

Privacy

- Common law has been developing a tort of "invasion of privacy", but it is not well-established.
  - Often only called upon for eavesdropping, trespass, etc.

4

History of Privacy Laws

- Public sector laws dated back 20+ years
  - *Privacy Act* – protection of personal information held by federal government
  - *Freedom of Information and Protection of Privacy Act* (NS) – protection of personal information held by the provincial governments
- No private sector laws until recently
  - Only Quebec!
- According to surveys, one significant impediment to widespread adoption of electronic commerce has been consumer privacy.
- Part of the federal government's e-commerce agenda, but not limited to online activities

5

Privacy - PIPEDA

- PIPEDA is implemented in a unique way that demonstrates its unusual constitutional position.
  - Property and civil rights in a province are part of **provincial** jurisdiction.
  - Privacy is a civil right.
  - But commerce is inter-provincial, international, inter-jurisdictional.
  - Some constitutional scholars say it is unconstitutional.
  - Government decided on a phased-in implementation.

6

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.

7

Privacy - PIPEDA

- Phased in application
  - 1 January 2001 - Federal Private Sector
    - Telecommunications, railways, air travel, shipping, credit bureaus, banks
  - 1 January 2004 - Provincial Private Sector
    - The rest of the economy
- Exemption if provincial government steps in and passes legislation that is declared to be "substantially similar".

No such legislation in Atlantic Canada – none anticipated

8

Privacy - PIPEDA

- Exclusions
  - Areas already covered by federal *Privacy Act*.
  - Domestic purposes – personal address book, Christmas card list
  - Information compiled for journalistic, artistic or literary purposes

9

Privacy - PIPEDA

- Addresses "personal information" – information about an identifiable individual:
  - **NOT** name, title, business address or telephone number of an employee or organization
  - Would include name, address, income, health information, demographics, preferences, birth date, SIN, customer numbers, unique identifiers
  - Also includes analysis or opinions about an individual
- Also includes information that may be traced back to an individual, including a credit score

10

Privacy Principles

- Based on the principles of the Canadian Standards Association Model Code for the Protection of Personal Information:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

11

Principles

1. **Accountability** - 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 principles contained in the Canadian Standards Association model code for the protection of personal information.
2. **Identifying Purposes** - the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent** - the knowledge and consent of the individual are required for the collection, or disclosure of personal information, except where inappropriate. Form of consent is dependent upon the sensitivity of the information

12

Principles

4. **Limiting Collection** - the collection of personal information shall be limited by that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention** - 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.

13

Principles

6. **Accuracy** - Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards** - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness** - An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

14

Principles

9. **Individual Access** - 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.
10. **Challenging Compliance** - 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.

15

Privacy – Obligations for Affected Businesses

- Appoint a privacy officer
- Make sure the privacy officer is well-trained
- Create and enact policies and practices to protect personal information in the business
- Create and enact policies and practices to receive and respond to complaints and inquiries from customers and the general public
- Create and enact policies and practices to train staff about the businesses policies and practices
- Create and enact policies and practices to enable staff to explain why specific information is being collected
- Communicate policies and procedures to customers
- Communicate purposes, uses and disclosures to customers
- Create consent forms for collection, use and disclosure of personal information
- Create contracts with service providers to follow the businesses' policies
- Create contracts with finance companies and others to allocate obligations with respect to financial information that is collected as part of financing purchases
- Ensure that informed consent is obtained for the collection and disclosure of personal information
- Put in place audit and disclosure records
- Protect personal information holdings with adequate security measures
- Keep up to date with changes to the law or interpretations of the law
- And more!

16

Does it apply to you?

- **Phased in:**
  - **January 1, 2001** – Federally-regulated sector
    - Are you subject to the *Canada Labour Code*? If yes, you are federally-regulated
    - Is personal information disclosed outside the province for consideration?
    - Do any of your "business lines" sell client lists?
  - **January 1, 2004** – Provincially-regulated private sector, unless the province in question has passed substantially similar legislation and the Governor-in-Council has exempted the province, activity, etc.
    - No Atlantic Canadian governments have expressed any intention to pass private sector privacy legislation.

17

Does it apply to you?

- *PIPEDA*, s. 4(1):

  "… applies to every organization in respect of personal information that

  (a) the organization collects, uses or discloses in the course of commercial activities; or

  (b) is about an employee of the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."

18

Does it apply to you?

- "... in the course of commercial activities... "
  - Defined in the Act to mean:

    "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund raising list"
  - Subject is the "**transaction, act or conduct**", not the whole enterprise
  - You can be non-profit, but engage in some commercial activities under the Act
    - E.g. universities operating bookstores, health clubs, etc.

19

Does it apply to you?

- The key is "commercial activities".
- Does not apply to personal information that is collected for artistic, journalistic and personal purposes (s. 4(2))
  - Christmas card lists
  - Personal address books

20

What about employees?

- PIPEDA only applies generally to employee information in the federally-regulated private sector
- Employee information is only covered in the provincially-regulated private sector if it is used in a commercial way

21

Consequences

- Individual (not just customer!) can make a written complaint to the Privacy Commissioner (s. 11).
  - Commissioner may initiate a complaint of his own accord.
  - Commissioner investigates the complaint
  - Powers in s. 12(1): Compel evidence, administer oaths, accept any evidence whether ordinarily admissible (or not), **enter any premises** other than a dwelling, review documents, etc.
- Commissioner's Report
  - To contain findings and recommendations, whether there was a settlement
  - Commissioner can decline to issue a report if the complainant has other recourse available

22

Consequences

- Court hearing
  - A complainant (***not the organization***), after receiving the Commissioner's report, may apply to the Federal Court – Trial Division for a hearing.
- Court's remedies include:
  - Order the organization to correct its practices in order to comply with ss. 5-10 of the Act;
  - Order the organization to publish a notice of actions taken to correct its practices; and
  - Award damages, including damages for humiliation the complainant may have suffered.

23

Powers of the Commissioner

- Audits (Division 3 of Part I)
  - On reasonable notice and at any reasonable time with reasonable grounds to believe the organization is contravening a provision of Division 1 or Schedule 1
  - Take evidence and enforce attendance as a superior court of record, even if not otherwise admissible in a court of law.
  - Enter any premises, other than a dwelling house
  - Examine or copy records or extracts of records

24

Concerns for Business

- High compliance burden
- Transfers between affiliates are caught by the Act
- Asset purchases are not covered
- Personal information does not have to be recorded to be subject of the Act
- Interpreted to cover analysis, opinion or conclusions based on personal information

25

Employers need to know

- PIPEDA creates a number of **offences** about which employers must be aware. It is unlawful to
  - discipline or retaliate against an employee or independent contractor who
    - "Whistleblows" to the Commissioner about the employer's privacy practices;
    - Refuses to do something contrary to Part I of the Act;
    - Acts to prevent a contravention of Part I of the Act;
  - Interferes with an investigation of the Commissioner
  - destroy personal information before a complainant has exhausted his/her recourse against the organization

26

Power of Publicity

- Commissioner has the power to "make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so." s. 20(2).
- Commissioner can publicize information handling practices, even before the Court has been given the opportunity to consider the matter.
- Commissioner's pronouncements are privileged for the purposes of any law related to libel or slander, so long as it is said in good faith.

27

What it means

- Significant impact on all businesses – disproportionate impact on small businesses.
- ***No grandfathering*** – any information collected before the Act comes into force for an organization can only be used if its collection and use are in compliance with PIPEDA. (e.g. consent, identified purpose, limited collection,etc.)
- Cannot "re-purpose" previously collected information without new consent.

28

PIPEDA and Credit Grantors

29

Does PIPEDA Apply?

- PIPEDA ***already applies*** for credit bureaus that transfer personal information across borders (provincial & national) for consideration
- As of January 1, 2004, PIPEDA will apply to all dealings with *personal* credit information

30

PIPEDA and Credit Grantors

- Remember the distinction between "personal information" and business information
  - Is it about an identifiable individual?
- Credit grantors require personal information to evaluate credit risks in order to approve credit
- Credit grantors also disclose personal information to third parties as a result of credit experience
- Credit-related info is ***sensitive*** information and consent is required for collection

31

PIPEDA and Credit Grantors

- Knowledge and consent of the individual is required: all aspects of collection, use and disclosure.
- Usually collect information directly from the individual such as:
  - Full name
  - Address (present and past)
  - Home ownership information
  - Immigration status
  - Employer
  - Job title
  - Income (sources and amount)
  - Student information (school, student #, etc.)
  - Assets

32

PIPEDA and Credit Grantors

- Usually confirm directly provided information and collect additional information about the individual
  - Credit report
    - Bankruptcies
    - Existing credit facilities
  - Confirm employment/income status
  - May search PPSA, judgments, etc

33

PIPEDA and Credit Grantors

- All of this is a collection of personal information for which the ***knowledge*** and ***consent*** of the individual are required.
- Credit grantors have to make reasonable efforts to disclose the purpose and obtain consent.
- Be careful what you demand …

34

Sample (very generic) disclosure

- In order to make a decision of whether to grant credit, the Company requires certain personal information from you and also needs to obtain information from other parties, such as consumer reporting agencies. We also may need to confirm information that you have provided to us. The Company limits the information that it collects and discloses to that which is reasonably necessary to provide you with the products or services that you have requested from us.
- I, the applicant, understand that in order to evaluate my credit application and to continue monitoring my ongoing credit status and eligibility for services, the Company is required to collect, use, maintain and disclose certain personal information about me. I hereby consent to the collection, use and disclosure of credit-related information about me with organizations such as employers, credit bureaus, credit grantors, and insurers. I understand that I may revoke this consent and I understand that if this consent is revoked, the Company will no longer be able to offer me any credit-related facilities and any amounts owing will be immediately due and payable. Notwithstanding any revocation, I agree that the Company may report the status of my account to credit bureaus.
- Providing your social insurance number (SIN) is **entirely optional**. Because credit bureaus commonly use the SIN as an identifier, providing your SIN may expedite the our ability to make a decision about whether to grant you credit. However, in no event will not providing your SIN be used to refuse you credit or services.

35

Consent Exceptions

- S. 7 contains exceptions to the general rule requiring consent.
- Disclosure without knowledge or consent

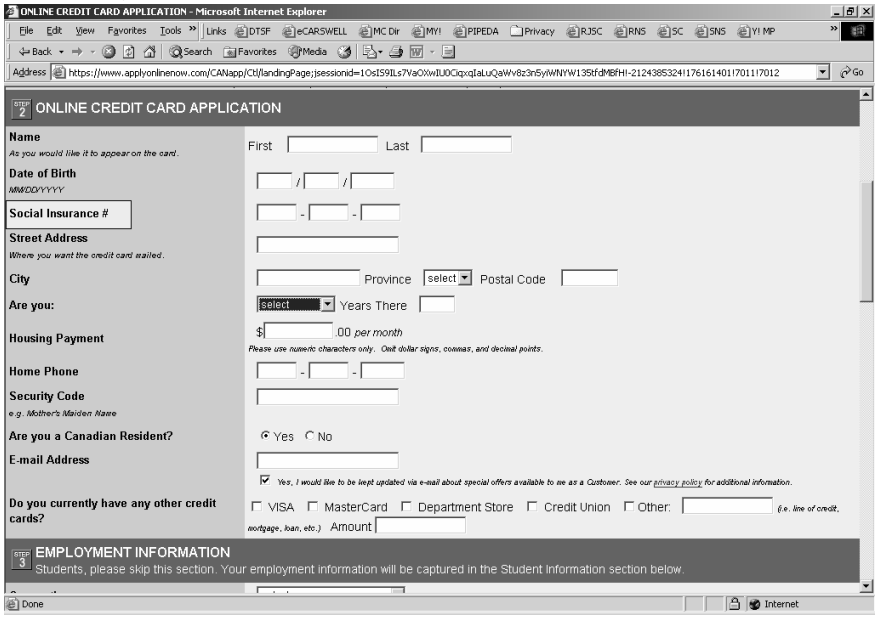
  7(3) For the purpose of clause 4.3 [Consent Principle] of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

  (*a*) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

  (*b*) for the purpose of collecting a debt owed by the individual to the organization; ...
- Other exemptions exist, but these are the prime concern for credit grantors

36

Social Insurance Numbers



Social Insurance Numbers

- Don't even ask!
- You can ask, but it has to be clearly optional.
- You cannot require an individual provide personal information that is not necessary for the service.
- Source of many complaints to the Office of the Privacy Commissioner.
- Findings are published at http://www.privcom.gc.ca.

38

Commissioner's Findings

- PIPEDA Case #115:
  - Back acquired the credit card business of another bank. New bank required SIN to activate a credit card
  - Individual refused to provide SIN, complained
  - Bank said SIN is the only "good unique identifier"
  - Finding:
    - Principle 4.3 states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Principle 4.3.2 elaborates on the matter of knowledge and consent by establishing that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.
    - Given the bank's uncertainty as to the circumstances of the original collection of the SINs and ***given that the purpose of identification was other than the primary legislated purpose of income reporting, the bank should have made a reasonable effort to inform its new customers about this new purpose and to obtain their consent***. The Commissioner could find no evidence that the bank had made such an effort or obtained customers' consent, and therefore found the bank in contravention of Principles 4.3 and 4.3.2 of Schedule 1 to the *Act*. ***He was, however, pleased that the bank had eliminated the use of the SIN for the purpose of activating a credit card***.

39

Commissioner's Findings

- PIPEDA Case # 166 – Bank refuses to provide loan because SIN not given
- Couple applied for loan and bank demanded SIN. Couple refused and loan application was turned down because of this.
- Couple complained to the Commissioner.
- Bank said that their policy was ***not*** to require the SIN and that customer service rep had made an error demanding it.
- Finding:
  - Principle 4.3.3 of Schedule 1 of the *Act* states that an organization must 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. Subsection 5(3) states that an organization may collect, use, or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.
  - The Commissioner noted that the use of the SIN has become widespread since it was first introduced in 1964. At the time, the SIN was created to serve as a customer account number in the administration of the Canada Pension Plan and Canada's varied employment insurance programs. In an effort to prevent the SIN from being used as a universal identifier, the federal government adopted a policy limiting the collection and use of the SIN by government institutions within the context of specific statutes, regulations and programs. ***Although there is no legislation preventing an organization from asking for the SIN for other purposes, mainly to identify a person, the Commissioner noted that organizations subject to the Act should clearly indicate to consumers that providing their SIN is optional and is not a condition for obtaining the service requested.***
  - Following the investigation, the Commissioner determined that the bank was ***not in compliance with Principle 4.3.3 because the SIN was not required for the loan application. As for subsection 5(3) of the Act, the Commissioner deems it unacceptable that the bank requires customers to provide a SIN to negotiate a loan. In addition, the bank did not correctly apply its policy according to which the SIN is optional and is not a condition of service***.

40

Commissioner's Findings

- PIPEDA Case # 85 - Customer questions credit rating assigned by bank
- Individual obtained car loan from bank. Believed that he had paid it off, but had not paid last installment, which was referred to collection.
- He was unable to obtain further loan because credit report indicated that "bad debt – referred to collection" was on his report.
- Applicant wanted the notation removed and sought correction of his credit report.
- Finding:
  - Principle 4.9 states that 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; and that the individual shall be able to challenge the accuracy and completeness of personal information and have it amended as appropriate. ***Principle 4.9.5 states that when an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required***.
  - The Commissioner determined that the complainant was able to challenge the accuracy of his personal information, as required by Principle 4.9. At that time, the ***amendment of his personal information was not required according to Principle 4.9.5 since the personal information on his credit bureau report was accurate, and based on common industry practice, the seven-year period had not yet expired***.
  - The Commissioner was satisfied that the bank had in fact been correctly reporting the complainant's personal information. Therefore, he did not find the bank to be in contravention of Principles 4.9 and 4.9.5 of Schedule 1 to the *Act*. 41

Commissioner's Findings

- PIPEDA Case #99 – Personal information improperly disclosed to collection agency
- Telephone company trying to trace a former customer who skipped out with a balance owing.
- Phone company hired a collection agency and provided them with the complainant's (unlisted) number, which was frequently called by the debtor.
- Phone company said that the number alone is not personal information.
- Finding
  - Section 2 of the *Act* defines personal information to be "...information about an identifiable individual...". Principle 4.3 states that knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Section 5(3) states that an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. Section 7(3)(b) of the *Act* states that for the purpose of clause 4.3 of Schedule 1, an organization may disclose personal information without the knowledge or consent of an individual only if the disclosure is for the purpose of collecting a debt owed by the individual to the organization.
  - ***The Commissioner concluded that the complainant's number was the personal information of both the complainant and the debtor***. The debtor was an identified individual in relation to the telephone numbers in his billing records, and thus the numbers could reasonably be deemed his personal information. The Commissioner noted, however, that the *Act* states only that the individual must be "identifiable," not that the individual be *identified*. It also does not say that the personal information must be unique to an individual. Though, the complainant was not identified by name in the records, his telephone number made it possible for him to be identified. Therefore, the Commissioner was satisfied that his telephone number was his personal information.
  - The Commissioner considered the customer's expectation that that his unlisted number would remain confidential, available only to employees of the telephone company and anyone else the individual chooses. It was clear that the complainant expected his number to remain confidential. While the company argued that it had the right to disclose this information without the complainant's knowledge or consent because it was pursuing the collection of a debt, ***the Commissioner noted that the company may only invoke such exceptions when it is attempting to collect on a debt owed by the individual whose information has been disclosed. The complainant's account was not at issue and the company had no basis on which to explain its disclosure of the complainant's personal information.*** The Commissioner therefore found that the company had failed to comply with section 7(3)(b) and was therefore in contravention of Principle 4.3.
  - A reasonable person would not consider the disclosure of personal information of one person to pursue the debts of another to be an appropriate purpose in the circumstances. 42

Compliance and Accountability Under PIPEDA

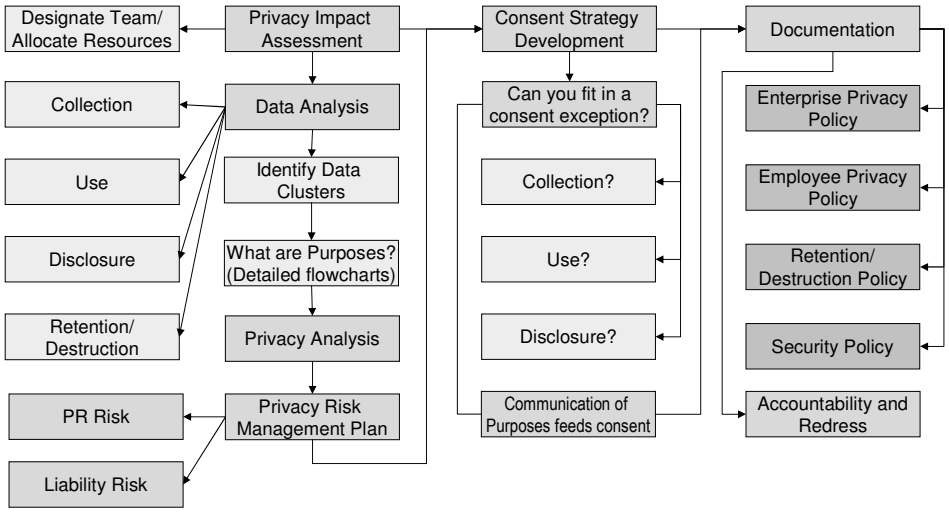
43

Existing Data / Processes

- Review existing data and new programs against all ten principles:
  - Direct collection or collateral?
  - Clear communication of purposes?
  - Are purposes reasonable?
  - Was consent obtained?
  - Capacity to consent?
  - Where is information held?
  - Who has access to it?
  - Any sharing (internal/external)?
  - Access for review?
  - Any derivative information?
  - Retention policy?
- Must remember – no grandfathering
  - Non-compliant data may not be used

44

Privacy Impact Assessment



45

Privacy Officer and Accountability

- Privacy Officer has three accountability responsibilities:
  1. Lead communications to the public/customers
  2. Resolve complaints
  3. Respond to investigations by the Commissioner
- Effectively implemented, accountability strategy will reduce risk to the organization by
  - Reducing complaints;
  - Addressing most complaints quickly and effectively before they go to the Commissioner or to Court; and
  - Resolve most complaints in a quiet way that preserves the reputation of the company.

46

Accountability under PIPEDA

- Applies to **every organization** that collects, uses or discloses personal information in the course of commercial activities.
- First Principle is accountability:
  1. **Accountability** - 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 principles contained in the Canadian Standards Association model code for the protection of personal information.

47

Accountability

4.1.4 Organizations shall **implement policies and practices** to give effect to the principles, including

(*a*) implementing procedures to **protect personal information**;

(*b*) establishing procedures to **receive and respond to complaints and inquiries**;

(*c*) **training staff** and communicating to staff information about the organization's policies and practices; and

(*d*) developing **information to explain the organization's policies and procedures**.

48

Privacy Officer

- The individual who is accountable for the organization's compliance with *PIPEDA*.
- Accountable to management, owners, board for the organization's compliance with the law **and** accountable to the public on behalf of the organization.
- Does not absolve the organization from ultimate responsibility
- Privacy Officer is unlikely to have any personal financial liability for organization's privacy practices

49

Communication

- Every organization is required to
  - Enact policies and procedures to implement the ten principles
  - Communicate to the public
    - what personal information is collected,
    - how it is used, and
    - with whom it is communicated.

50

Privacy Officer

- Public face of your organization's privacy law compliance
  - Not just a *pro forma* legal requirement
  - Key to showing respect to your customers/stakeholders
- Auditor – periodically reviews the organization's compliance with its own policies
- Resource
  - keeps up to date on privacy law as it relates to the organization
  - acts as a resource to management and other employees

51

Privacy Officer and Employees

- Many of the 200+ decisions from the Office of the Privacy Commissioner should not have gotten to that stage
  - many result from poor training of employees or poor handling of customers' legitimate concerns
- Communicate with your customers so they don't have privacy-related questions
  - tell them everything they'd want to know
- Answer any questions before they become complaints!
- Address complaints before they are escalated to the Office of the Privacy Commissioner!

52

Privacy Officer and Employees

- Enacts and enforces policies
- Need to train employees
  - All "front line employees" must
    - understand the company's privacy policies
    - be able to answer privacy-related questions
    - know how to build trust, not arouse suspicion

53

Build Trust With Your Customers

- Assume your customers are paranoid and suspicious
- Assume your customers want you to earn their trust
  - Anticipate concerns
  - Anticipate queries
  - Anticipate complaints
- Solve them before a customer has to deal with it and show them how you can be trusted

54

Dealing with Inquiries

- Provide prompt, honest answers
- Train employees to say what they know and escalate the matter very quickly to a superior
  - Sends the message that the company takes privacy seriously
  - Reduces the likelihood that a misunderstanding will arise
- "Customer is always right" – cliché that should serve you well
  - Unless it is a matter of principle (or huge cost!) try to accommodate the customer

55

Providing Access to Information

- Any individual has the right to know about whether the organization has personal information related to the individual
- If there is any personal information under control of the organization, individual has right of access to his/her personal information – within 30 days!
- Company needs to be able to have mechanism to accomplish this

56

Providing Access to Information

- Be prepared!
  - Know where you have information – from your information inventory
  - Know where to look, who to query
  - Make sure Privacy Officer has enough pull to require necessary assistance
- Get the right information from the individual to assist in the search
  - Name, address, any personal identifiers, dates of interaction with the organization, etc.
  - This information can only be used to assist in the search – cannot be used for any secondary purpose

57

Providing Access to Information

- Carefully vet materials before release
  - Are they easily understandable? Full of jargon, abbreviations?
    - Consider having "translation" resources if materials are usually not in plain English
  - Make sure that there is no **third-party personal information** included in the materials to be released
    - Can third-party info be excised?
    - Has third-party consent been obtained?
  - Make sure info is not subject to **solicitor-client privilege** or litigation privilege
  - Make sure info does not reveal **confidential business information** (reasonable definition)
- If difficulty with the above, consult counsel. You don't want to accidentally waive privilege

58

Providing Access to Information

- There are various ways of providing access to information
  - View originals on the organization's premises (needs space and supervision)
  - Provide photocopies or print-outs (costs of copying)
- Cost-recovery
  - Statute allows you to charge a reasonable fee for access
  - Suggest that you provide access for free
    - Communicates to customers that you want to assist them in exercising their important rights
    - If you charge, may build perception that the charge is there to discourage
  - Small charge may discourage frivolous or persistent inquirers
    - E.g. free copy of customer file every twelve months – discourages someone who asks every month
  - You will probably never recover your total costs of privacy-law compliance

59

Dealing with Complaints

- At the time of complaint, your job is to keep the customer's trust and to prevent a complaint
- Be the customer's advocate and let the customer know you're on his/her side
- Give prompt attention
  - Investigate quickly and thoroughly
  - If it will take some time to respond, let the customer know
    - Updates provide reassurance
- Do not appear to be merely defending the organization
- If it does not appear to be going well, consult with counsel as soon as possible

60

Dealing with Complaints

- If the organization is "at fault", provide a reasonable remedy
- Reasonable remedy will depend upon the particular circumstances
  - In many cases, sorry is all they want to hear
  - Will probably want to know what is being done to prevent a recurrence
  - If appropriate, offer reasonable compensation without accepting liability
- Place "without prejudice" on correspondence
  - In most cases, settlement discussions cannot be brought as evidence

61

Settling Complaints

- If trust-building is an issue, consider bringing in an impartial third-party to mediate
  - May cost $$$, but probably cheaper than a complaint to the Commissioner
  - Privacy Officer should not represent the organization in this mediation as the appearance of impartiality should be preserved
- If it is a significant complaint, get a settlement in writing
  - But may not prevent a complaint to the Commissioner or to the Court

62