Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?

April 2006

Canadian Internet Policy and Public Interest Clinic
Faculty of Law / University of Ottawa
57 Louis Pasteur, Room 506
Ottawa (ON) K1N 6N5

ACKNOWLEDGEMENTS

CIPPIC gratefully acknowledges the financial support of the Office of the Privacy Commissioner of Canada and the Social Sciences and Humanities Research Council for this study.

The study was directed by Philippa Lawson, Executive Director and General Counsel of CIPPIC, and coordinated by Jennifer Seligy, student-at-law. Annie Binet provided administrative support.

The following law students conducted assessments and/or submitted access requests: Anne Ko, Brian Harvey, Christopher Deeble, Damien Fox, David Lam, Dixie Ho, Dyna Lou, Grace Skowronski, Ioulia Vinogradova, Karen Poon, Kathy-Anne Chin Quee, Katrina Marciniak, Lara McGuire, Lukasz Kuzio, Michael Leach, Nyall Engfield, Rhoderica Chan, Shane O'Herlihy, Steven Choi, Suzanne Orsborn, Tanya Woods, Thomas Legault.

Jennifer Seligy analysed and compiled the assessment results. The report was drafted by Jennifer Seligy and edited by Philippa Lawson.

EXECUTIVE SUMMARY

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") was introduced in 2001 to protect Canadians from inappropriate collection, use and disclosure of their personal data by organizations in the course of commercial activities. Five years later, it is not clear to what extent organizations are in fact respecting the legislation. This study was designed to shed some light on that question, by assessing the compliance of retailers with certain key provisions of PIPEDA.

We assessed the compliance of 64 online retailers with the PIPEDA requirements for openness, accountability and consent. We also assessed the compliance of 72 online and offline retailers with the PIPEDA requirement for individual access. The results of our assessment indicate widespread non-compliance in all four areas.

While almost all companies we assessed had a privacy policy and were thus aware of the need to respect customer privacy, many failed to fulfill even basic statutory requirements such as providing contact information for their privacy officers, clearly stating what they do with consumers' personal information, and responding to access to information requests. A significant proportion of the policies we examined were unclear on key points such as whether or not consumer information is shared with other companies. Many failed to provide a clear and conspicuous method for consumers to opt-out of unnecessary uses and disclosures of their personal information, often relying on a clause buried deep in a lengthy privacy policy that consumers are unlikely to review.

A number of policies we examined were misleading, suggesting for example that no secondary use or sharing of personal information would take place without the consumer's explicit consent, but then assuming such consent unless the consumer exercised an often inconspicuous or incomplete opt-out.

The following are key findings from the compliance assessments:

GENERAL PRACTICES

- Almost all online retailers have privacy policies (94% of our sample), and most post them on their websites (92%).
- Privacy policies tend to be lengthy: 63% of those in our sample were over 1000 words long, and 35% were over 2000 words long.
- The vast majority of online retailers (at least 93% of our sample) use personal consumer information ("consumer information") for their own marketing purposes.
- A large proportion of online retailers (1/2 to 2/3 of our sample) share consumer information with other companies for purposes beyond those necessary for the transaction or service in question. Only one-third of our sample stated that they do not do so.
- Only one of the 29 companies in our sample that admitted to sharing consumer information with other organizations restricted its data-sharing to affiliates.
- A large majority of retailers (78% of our sample) rely on opt-out methods to obtain consumer consent to secondary uses or disclosures of their personal information.

PRINCIPLE 4.1 – ACCOUNTABILITY

- Online retailers are doing a poor job of ensuring that front-line staff are aware of the existence of the privacy policy, know who is responsible for it, and can direct inquirers to both the policy and the responsible officer. 68% of companies we contacted took over five minutes, and 22% took over ten minutes, to answer the questions: “Do you have a privacy policy?”, “How can I get it?” and “Who in your company is responsible for privacy matters?”
- 56% of companies we contacted by phone could not provide the name of an individual responsible for privacy when asked. Moreover, 30% of privacy policies we reviewed did not provide contact information for a person responsible for compliance with the policy.
- Few of the retailers we tested (only 14%) provided consistent contact information for designated privacy officers in their privacy policies and over the phone.

PRINCIPLE 4.8 - OPENNESS

- It is unreasonably difficult for consumers to acquire information over the phone about companies’ policies and practices with respect to the management of personal information. As noted above, 68% of companies we contacted took over five minutes, and 22% took over ten minutes, to answer the questions: “Do you have a privacy policy?”, “How can I get it?” and “Who in your company is responsible for privacy matters?”
- Four companies (6%) in our sample had no privacy policy whatsoever.
- While most online retailers make their privacy policies accessible online, 63% of companies in our sample could not or would not provide a copy by mail, fax or email when requested to do so.
- A significant proportion of privacy policies fail the test of clarity, even when tested by people with university education. Although 87% of policies reviewed were considered “generally understandable” by Assessors, many fewer were found to be clear on key points once Assessors looked more closely. Specifically, Assessors found that companies were unclear about the purpose of collection in 22% of cases, about what personal information they collect in 27% of cases, about how they use the information in 30% of cases, and about to whom they disclose the information in 45% of cases.
- An even higher proportion of privacy policies were incomplete:
    - 30% did not provide contact information for a privacy officer;
    - 38% made no reference to the consumer’s right to access his or her personal information held by the company;
    - 27% did not describe the type of consumer information held by the company;
    - 18% did not describe what the company does with consumer information;
    - 34% of those that admitted to sharing consumer information with other organizations did not describe the type of information that they share;
    - 86% of those that admitted to sharing did not indicate with whom they share consumer information; and the remaining 14% provided examples only.

PRINCIPLE 4.3 – CONSENT

- Not surprisingly, the vast majority of online retailers we surveyed (78%) rely on opt-out methods, at least in part, to obtain consumer consent for secondary uses and disclosures of their personal information. Only 8% use opt-in methods exclusively, and a surprising 14% do not bother to get consent through any means when customers register or order on their site, even though they admit to secondary uses or disclosures or are unclear on this point.
- Under PIPEDA, consent must be informed. Yet, 17% of the privacy policies reviewed were unclear about whether the company uses consumer information for marketing purposes, and 18% were unclear about whether the company shares consumer information with other companies. A further 6% of companies did not have privacy policies at all. In 31% of the cases we reviewed, the companies provided no notice via the privacy policy or otherwise during the registration or ordering process.
- Moreover, during the registration or ordering process, the majority of the 64 companies we assessed (53%) provided notice to customers only via a link to the privacy policy, requiring consumers to visit the privacy policy and read through it for an understanding of what the company does with their personal information. Of these, 56% failed to bring the link to the privacy policy to the customer's attention during the registration or ordering process.
- We found a number of misleading privacy policies. In particular, of the 60 privacy policies assessed, 18% suggest that the company uses opt-in consent when in fact it relies on opt-out consent. This misleads consumers into thinking that their information will not be used for secondary purposes when in fact it will.
- Twenty-nine companies (48% of our sample) admitted to sharing consumer information with other companies for purposes other than the transaction in question (another 11 (18%) were unclear). Yet, ten of these companies (34% of those that clearly share) did not offer consumers a choice regarding this practice during the registration or ordering process.
- The methods used by many online retailers to obtain consent from consumers do not meet the requirements for valid consent.
    - Of those companies relying on opt-out consent, 50% did so merely via a link to an often lengthy privacy policy as part of the registration or ordering process. In these cases, the majority (52%) failed to bring the link to the privacy policy to the customer's attention.
    - Of those companies that included an opt-out in their privacy policy, 60% buried it inconspicuously in the often lengthy policy.
    - Ten companies in our sample offered fewer opt-out options during the registration or ordering process than via their privacy policies, without any indication to consumers that additional opt-out options were available via the privacy policy. This misleading practice was exacerbated by the fact that none of these companies bothered to bring their privacy policy to the attention of consumers during the registration or ordering process.
    - Of those companies relying on opt-out consent, 50% did not offer an immediate opt-out option as part of the transaction; rather, consumers have to consent against their will initially and then take additional steps to opt-out.

- In seven cases (11%), the retailer clearly required consent to a secondary purpose in order for the consumer to transact. In none of these cases did the consumer receive any value in exchange for such consent. In an additional 18 cases, Assessors were not sure whether consent to a secondary use or disclosure was mandatory, due to lack of clarity in the privacy policy or an absence of a written privacy policy. Thus, potentially 39% of companies we assessed are violating PIPEDA's "refusal to deal" section.

PRINCIPLE 4.9 – INDIVIDUAL ACCESS

- A large proportion of companies are failing to comply with the PIPEDA requirement to inform individuals of the existence, use and disclosure of their personal information upon request, and to give individuals access to that information.
- One-third (35%) of the companies we tested did not respond at all to access requests.
- Of the companies that did respond,
    - 42% failed to provide details about the Requestor's personal information they had on file;
    - 37% provided no account or an inadequate account of how they use the personal information; and
    - 58% did not give a list of companies to whom they have or may have disclosed personal information about the Requestor;

  despite being specifically asked for this information by the Requestor.

TABLE OF CONTENTS

INTRODUCTION

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") was introduced in 2001 to protect Canadians from inappropriate collection, use and disclosure of their personal data by organizations in the course of commercial activities. It is not clear however, to what extent such organizations are in fact respecting the legislation. To our knowledge, no study has yet been conducted to confirm the extent to which organizations subject to PIPEDA are complying with it.

With privacy protection increasingly becoming one of Canadians' top concerns and the five-year Parliamentary Review of PIPEDA scheduled for the fall of 2006, the time is ripe for testing of private industry compliance with PIPEDA. Such testing can contribute to a more informed Parliamentary review of PIPEDA, as well as provide a useful tool for holding companies accountable under PIPEDA and thus making Canadian privacy laws more effective.

It was within this context that the Office of the Privacy Commissioner of Canada provided funding under its 2005-2006 Contributions Program to the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") to evaluate organizational compliance with PIPEDA.

SCOPE AND SAMPLES

This report assesses the policies and practices of 64 online retailers[1] with respect to PIPEDA provisions covering Accountability, Openness and Consent. Of the 64 retailers examined, 42% were large, 20% were medium-sized, 24% were small, and 3% had fewer than five employees. Seven companies in our sample refused to provide us with information about their size.

Table 1: Sample by Company Size

Company Size (self-identified by company)	Company Responses	Percentage
Micro (1-4 employees)	2	3%
Small (5-49 employees)	15	24%
Medium (50-499 employees)	13	20%
Large (500+ employees)	27	42%
Unknown (company did not want to provide company size)	7	11%

This report also assesses the practices of a separate sample of 72 online and offline retailers with respect to Individual Access rights under PIPEDA. Although there is some overlap, this sample is different from the former sample given the nature of testing required for Individual Access.

OBJECTIVES

This study has the following goals:

- To assess the extent to which retailers are complying with PIPEDA requirements for Openness, Accountability, Consent and Individual Access;
- To develop a tool for assessing compliance and holding companies accountable under PIPEDA; and
- To identify problems in the interpretation/application of PIPEDA that could be resolved through amendments to PIPEDA.

[1] Both goods and service providers.

RESEARCH METHODOLOGY

This study focuses on those obligations under PIPEDA that can be tested either by calling the company's main telephone number, by writing to the company, or by reviewing the company's privacy policy and ordering practices. CIPPIC conducted a series of pre-tests on a variety of PIPEDA principles and ultimately settled on testing Principle 4.1 (Accountability), Principle 4.8 (Openness), Principle 4.3 (Consent), and Principle 4.9 (Individual Access). Assessment guides and questionnaires were drafted, tested, and revised over the course of three months (October to December 2005) before being finalized.

CIPPIC developed one methodological approach for testing Principles 4.1, 4.3 and 4.8, and another for Principle 4.9. Each is described below.

COMPLIANCE WITH ACCOUNTABILITY, OPENNESS AND CONSENT

Assessors

Eleven University of Ottawa law students acting as ordinary consumers ("Assessors") conducted assessments of 64 companies' privacy policies and practices over a three month period from January to March 2006. Assessors performed each assessment in part by calling the company's general telephone number, in part by reviewing the company's privacy policy, and in part by analyzing the company's ordering practices. All Assessors underwent training sessions of approximately two hours prior to conducting their assessments. Training consisted of a tutorial on PIPEDA followed by an overview of the PIPEDA Compliance Testing project and a sample assessment.

Survey Sample

To avoid bias in the selection of companies for testing, CIPPIC used two externally compiled lists from which to draw its survey sample: one containing a list of online retail, travel, and ticketing services [2] ("Directory 1") and another with a list of magazines sold online [3] ("Directory 2").

From Directory 1, all of the companies listed in the "Major Retailers" category, and all of the companies listed under the first subheadings in the "Health/Beauty", "Computers", "Electronics", "Books/Music/Movies", "Sporting Goods", "Travel/Vacation" (except for the luggage stores) and "Other Retailers" categories were selected and placed on a master list in the same order as they appear in the Directory. From Directory 2, all the magazines listed on the first two pages in the "Magazines" section were selected and added to the master list in the same order as they appear in the Directory.

Any company that appeared more than once on the master list, that was no longer in operation, or that did not allow for online transactions was removed from the list. The final master list (Appendix A) contained 64 companies. Assessors were assigned companies from this list beginning with the first company on the list and working down the list. The number of companies assigned to each Assessor varied depending on the amount of time the Assessor was available for participation in the study. Each company in the survey was contacted and asked to self-identify as being either micro (1-4 employees), small (5- 49 employees), medium (50-499 employees) or large (500+ employees) (Appendix B).

Of the 64 companies in the survey sample, Assessors were unable to reach five companies by telephone to conduct the phone assessment portion of the study. This left 59 companies available for the phone assessment portion of the study.

Of the 64 companies in the sample, Assessors found that 59 companies post privacy policies on their websites. Of the five companies who do not post privacy policies online, one supplied its privacy

[2] Available online at: http://www.davidjohnson.ca/html/onlineshopping.shtml
[3] Available online at: http://www.canadaretail.ca/

policy by fax, while the remaining four could not supply a written privacy policy because they had none. As a result, a total of 60 companies' privacy policies were available for assessment.

All of the 64 companies in the survey sample provide online ordering services. Assessors were therefore able to test online ordering practices of all 64 companies.

Assessment Review and Tabulation of Results

Assessors recorded their results on a standard Form (Appendix C) and submitted them to the project coordinator ("the Coordinator") for review and entry into a database. The Coordinator reviewed all assessments to make sure that Assessors recorded answers correctly. The Coordinator corrected factual errors, but did not change any of the Assessors' responses to subjective questions, even where the Coordinator disagreed with Assessors' answers. Results were inputted into a database, and correlations were done manually.

COMPLIANCE WITH INDIVIDUAL ACCESS

Requesters

Four CIPPIC staff members and 17 University of Ottawa law students ("Requesters"), in their personal capacities, conducted access requests for this study. Requesters used a template letter for their requests (Appendix D) and an assessment form to record the results of their requests (Appendix E). Requesters conducted access requests in two phases: February - June 2005, and November 2005 - February 2006.

Survey Sample

Requesters were asked to submit access requests to companies with whom they had done business. All the companies that Requestors volunteered to contact were recorded on a master list of companies and organized by sector (Appendix F). Where more than one request was made of a company, only the first request was used for this study. Otherwise, all requests were recorded and used in the study.

Assessment Review

The Coordinator reviewed all assessment forms for accuracy and entered the information contained in the Forms into a database. Ultimately, 72 access requests were made to 72 different companies.

FINDINGS UNDER PIPEDA

PART 1: COMPLIANCE WITH ACCOUNTABILITY, OPENNESS AND CONSENT

GENERAL PRACTICES

Key Findings

Almost all online retailers have privacy policies (94% of our sample), and most post them on their websites (92%).

Privacy policies tend to be lengthy: 63% of those in our sample were over 1000 words long, and 35% were over 2000 words long.

The vast majority of online retailers (at least 93% of our sample) use personal consumer information ("consumer information") for their own marketing purposes.

A large proportion of online retailers (1/2 to 2/3 of our sample) share consumer information with other companies for purposes beyond those necessary for the transaction or service in question. Only one-third of our sample stated that they do not do so.

Only one of the 29 companies in our sample that admitted to sharing consumer information with other organizations restricted its data-sharing to affiliates.

A large majority of retailers (78% of our sample) rely on opt-out methods to obtain consumer consent to secondary uses or disclosures of their personal information.

Privacy Policies

Of the 60 privacy policies reviewed, 37% were less than 1000 words, 28% were between 1000 and 2000 words, and 17% were over 3000 words in length. In most cases (83%) Assessors found the privacy policies to be contained in a single document, however, there were a number of cases (17%) where Assessors had to follow links to other documents to fully understand the companies' information management practices.

Table 2: Privacy Policies

How long is the privacy policy (in words)?	Assessor Responses	Percentage
1 - 500 words	10	17%
500 - 1000 words	12	20%
1000 - 2000 words	17	28%
2000 - 3000 words	11	18%
Over 3000 words	10	17%
N/A: Company has no written privacy policy	4	N/A

Of the 59 companies who post privacy policies on their websites, a majority (70%) provide a link to the policy in small font with other links at the bottom of the homepage and 24% provide a link to the privacy policy on a menu bar at the top or side of the homepage. Six companies provide a privacy link on their homepages only; most companies include the link to the privacy policy on other pages in addition to the homepage.

Internal Marketing

Most companies (83%) state in their privacy policies that they use consumer information for their own marketing purposes. Six companies (10%) do not state that they use consumer information for internal marketing purposes, but do use opt-in or opt-out during the registration or ordering process to obtain consumer consent to use their personal information for internal marketing. This brings the total number of companies who use consumer information for these purposes to 93%. However, actual use of consumer information for internal marketing purposes may be as high as 100% because in the remaining four cases, Assessors found privacy policies to be unclear on this point.

Table 3: Internal Marketing

According to the privacy policy, does the company use consumer information for its own marketing purposes?	Assessor Responses	Percentage
Yes	50	83%
No	0	0%
Unclear, but company asks consumers to opt-in or opt-out to internal marketing during registration/ordering	6	10%
Unclear	4	7%
N/A: Company has no written privacy policy	4	N/A

Sharing with Other Companies

Assessors found that a significant proportion of companies (48%) admit to sharing consumer with other companies for purposes other than the transaction or service in question. In 34% of cases, companies stated that they do not share consumer information with other companies except as necessary for the transaction or service in question. The remaining 18% of policies were unclear on this point. Hence, actual sharing of consumer data with other companies could be as high as 66%.

Table 4: Sharing with Other Companies

According to the privacy policy, does the company share consumers' personal information with other companies for purposes other than the transaction or service in question?	Assessor Responses	Percentage
Yes	29	48%
No	20	34%
Unclear	11	18%
N/A: Company has no written privacy policy	4	N/A

Of the 29 companies who admit to sharing consumers' personal information with other companies for secondary purposes, Assessors found that only one company limits its sharing to affiliates.

Table 5: Sharing with Affiliates and Third Parties

According to the privacy policy, with whom does the company share consumers' personal information?	Assessor Responses	Percentage
Affiliates only	1	4%
Third parties only	14	48%
Both affiliates and third parties	14	48%

Opt-in vs. Opt-out Consent

Assessors reported that of the 64 companies in the survey sample, the vast majority (78%) use an opt-out method during the registration or ordering process to obtain consumer consent to at least some secondary uses and disclosures of consumers' information. Only five companies (8%) use opt-in exclusively, and nine (14%) do not use opt-in or opt-out consent during the registration or ordering process, even though they either admit to secondary uses or disclosures or are unclear on this point.

Online Ordering Practices

A significant proportion (41%) of the 64 companies assessed require customers to register with the company before they can place an order. In six (9%) of these cases, customers are asked to consent (or withdraw deemed consent) to secondary uses or disclosures of their personal information during the registration process only.

Table 6: Online Ordering Practices

Registration vs. Ordering	**Number of Companies**	**Percentage**
Registration required before ordering	26	41%
No registration required	38	59%
Opt-in / Opt-out Option		
Opt-out during registration only	3	5%
Opt-out during both registration and ordering	19	30%
Opt-out during ordering only	23	36%
Opt-out and opt-in during ordering	5	7%
Opt-in during registration only	3	5%
Opt-in during ordering only	2	3%
No opt-out or opt-in during registration or ordering	9	14%

FINDINGS FOR PRINCIPLE 4.1 – ACCOUNTABILITY

Key Findings

Online retailers are doing a poor job of ensuring that front-line staff are aware of the existence of the privacy policy, know who is responsible for it, and can direct inquirers to both the policy and the responsible officer. 68% of companies we contacted took over five minutes, and 22% took over ten minutes, to answer the questions: "Do you have a privacy policy?", "How can I get it?" and "Who in your company is responsible for privacy matters?"

56% of companies we contacted by phone could not provide the name of an individual responsible for privacy when asked. Moreover, 30% of privacy policies we reviewed did not provide contact information for a person responsible for compliance with the policy.

Few of the retailers we tested (only 14%) provided consistent contact information for designated privacy officers in their privacy policies and over the phone.

Designated Privacy Officer

Principle 4.1 requires that:

> *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 foregoing principles.*

Principle 4.1.2 further requires that:

> *The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.*

To test these elements of accountability, Assessors, acting as ordinary customers, phoned each company's general customer service number and asked whether the company had a designated individual responsible for handling privacy inquiries and/or complaints, and for that individual's contact information. In five cases, Assessors were unable to reach a person at the company by phone, despite repeated efforts.

Of those that could be reached, a majority (56%) replied that they did not have a designated individual who is accountable for the organization's privacy policies and practices, although 70% of the companies name such a person in their privacy policies (see Table 15).

Table 7: Designated Privacy Officer

Do you have someone that is responsible for handling privacy inquiries/complaints?	Company Responses	Percentage
Yes (contact information provided)	26	44%
No	33	56%
N/A: Assessor unable to reach anyone at the company by phone	5	N/A

Staff Training

Principle 4.1.4 states:

> *Organizations shall implement policies and practices to give effect to the principles, including*
>
> *…(c) training staff and communicating to staff information about the organization's policies and practices.*

To test this principle, Assessors phoned each company's general customer service inquiry number and asked (a) whether they have a privacy policy and (b) how to get a copy of the privacy policy.

While the majority of companies contacted (91%) ultimately responded 'Yes' to the question of whether or not they had a privacy policy, a significant number of company representatives (32%) only responded positively to the question after prompting from the Assessor. In these instances, Assessors had to explain what a privacy policy is before the company representative could answer the question.

Table 8: Does the Company Have a Privacy Policy

Do you have a privacy policy?	Company Responses	Percentage
Yes	35	59%
Yes, but only after Assessor explained what a privacy policy is	19	32%
No	5	9%
N/A: Assessor unable to reach anyone at the company by phone	5	N/A

When asked where customers can obtain a copy of the privacy policy, most company representatives (78%) referred Assessors to the company website.

Assessors also asked each company representative for the name and contact information of a person responsible for handling privacy-related inquiries. Assessors then compared this information to the contact information supplied in the privacy policy. Of the 26 company representatives who supplied Assessors with contact information over the phone (see Table 7), only eight (31%) provided the same contact information that appears in the company's privacy policy.

Table 9: Contact Information for Company Privacy Officer

Is the contact information supplied in the privacy policy the same as the contact information supplied by the company representative?	**Assessors Responses**	**Percentage**
Yes	8	31%
No	18	69%
N/A: Can't compare because company representative did not supply contact information upon request	33	N/A
N/A: Assessor unable to reach anyone at the company by phone	5	N/A

Ultimately, of the 59 companies contacted, only 8 (14%) provided consistent contact information for the individual responsible for handling privacy matters both in their privacy policies and upon request.

FINDINGS FOR PRINCIPLE 4.8 - OPENNESS

Key Findings

It is unreasonably difficult for consumers to acquire information over the phone about companies' policies and practices with respect to the management of personal information. As noted above, 68% of companies we contacted took over five minutes, and 22% took over ten minutes, to answer the questions: "Do you have a privacy policy?", "How can I get it?" and "Who in your company is responsible for privacy matters?"

Four companies (6%) in our sample had no privacy policy whatsoever.

While most online retailers make their privacy policies accessible online, 63% of companies in our sample could not or would not provide a copy by mail, fax or email when requested to do so.

A significant proportion of privacy policies fail the test of clarity, even when tested by people with university education. Although 87% of policies reviewed were considered "generally understandable" by Assessors, many fewer were found to be clear on key points once Assessors looked more closely. Specifically, Assessors found that companies were unclear about the purpose of collection in 22% of cases, about what personal information they collect in 27% of cases, about how they use the information in 30% of cases, and about to whom they disclose the information in 45% of cases.

An even higher proportion of privacy policies were incomplete:

- 30% did not provide contact information for a privacy officer;
- 38% made no reference to the consumer's right to access his or her personal information held by the company;
- 27% did not describe the type of consumer information held by the company;
- 18% did not describe what the company does with consumer information;

- 34% of those that admitted to sharing consumer information with other organizations did not describe the type of information that they share;
- 86% of those that admitted to sharing did not indicate with whom they share consumer information; and the remaining 14% provided examples only.

Making Information Available

Principle 4.8. states that:

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

Principle 4.8.1 further requires that organizations:

> *Be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.*

According to the Privacy Commissioner, making information "readily available", includes making privacy policies available to the public in a variety of ways. This is particularly important for those who do not have Internet access.[4]

To test compliance, Assessors reported the time and level of difficulty required to find out: (a) if the company had a privacy policy; (b) how it could be obtained; and (c) who in the company deals with privacy matters. The survey sample for this testing comprised 59 companies, since five companies could not be reached by phone.

In 68% of cases, Assessors had to spend over five minutes on the phone before they could get answers to their questions. In 13 cases (22%), Assessors had to spend more than ten minutes on the phone. It is also worth noting that while in most cases Assessors reported that it was easy to get answers, often those answers were inconsistent with the privacy policy (see Table 9).

Table 10: Time Spent on Phone

How long were you on the phone before you got answers to the following questions: **Do you have a privacy policy?** **If yes, how can I access it?** **Do you have someone responsible for handling privacy inquiries?**	**Assessor Responses**	**Percentage**
1 - 5 minutes	19	32%
5 - 10 minutes	27	46%
10 - 15 minutes	8	13%
15 - 20 minutes	4	7%
20 - 25 minutes	1	2%
N/A: Assessor unable to reach anyone at the company by phone	5	N/A

When Assessors asked if they could obtain a copy of the privacy policy by fax, email or mail, a majority of companies (63%) responded that this was not possible even when Assessors claimed not to have Internet access. The most common reason cited for the inability to furnish the privacy policy by mail, fax, or email was that the privacy policy is only available by printing it off the website. This reason was given in 57% of the cases where the company representative refused to supply the

[4] Privacy Commissioner Finding #304, June 7, 2005 <http://www.privcom.gc.ca/cf-dc/2005/index2-5_e.asp>

privacy policy by mail, fax or email. These findings indicate a general unwillingness on the part of most companies in the sample to furnish their privacy policies in more than one format.

Table 11: Availability of privacy policy in a different format

Can I obtain a hard copy of the privacy policy by fax, mail or email?	Company Responses	Percentage
Yes	22	37%
No	37	63%
N/A: Assessor unable to reach anyone at the company by phone	5	N/A

Assessors also recorded whether they were able to understand the information about the company's data management policies and practices without unreasonable effort both over the phone and in the course of the online assessment of the companies' privacy policies and ordering practices. In addition, Assessors timed how long it took, overall, to assess companies' privacy policies and online ordering practices. No restrictions were placed on the Assessors' time to complete each assessment, rather Assessors were encouraged to take all the time they needed to fully understand the company's information management practices.

Assessors reported that they were unable to understand the company's data management practices and policies without unreasonable effort in 31% of cases. In addition the majority of assessments (76%) took Assessors between 1 and 2.5 hours to complete. This represents a considerable amount of time spent trying to understand companies' basic information management practices, an amount of time that is likely far greater than any consumer would spend on their own attempts to understand a company's policies and practices regarding their personal data.

Table 12: Information About Privacy Practices

In general would you say that you were able to understand the company's data management policies and practices without "unreasonable effort"?	Assessor Responses	Percentage
Yes	44	69%
No	20	31%
How long did it take you to get answers to questions about the company's information management practices (website assessment only)?		
Less than 1 hour	11	17%
1 - 1.5 hours	25	39%
2 - 2.5 hours	24	37%
3 - 3.5 hours	3	5%
4 hours	1	2%

Availability of Privacy Policies

Of the 64 online retailers tested in the survey sample, Assessors found that five did not post privacy policies on their websites, and four of these five (6%) had no written policy at all. Of those with privacy policies online, most (70%) link to the policy only via a link in small font at the bottom of the webpage.

Clarity of Privacy Policies

Assessors were asked to review the companies' privacy policies and to answer the question "is the privacy policy clearly worded and generally understandable?", followed by a series of specific questions to measure Assessors' ability to determine what the company does with consumer information.

While only 13% of policies reviewed failed the "generally understandable" test, many more failed the test of intelligibility once Assessors dug deeper. In 27% of cases, Assessors found it difficult to determine what personal information the company collects; in 22% of cases, Assessors found it difficult to determine why the company collects personal information; in 30% of cases, Assessors found it difficult to determine how the company uses consumers' personal information; and in 45% of cases, Assessors found it difficult to determine to whom the company discloses consumers' personal information.

Table 13: Clarity of Privacy Policy

Is the privacy policy clearly worded and "generally understandable"?	**Assessor Responses**	**Percentage**
Yes	52	87%
No	8	13%
N/A: Company has no written privacy policy	4	N/A

Table 14: Assessors Understanding of the Privacy Policy

Is it easy to determine from the privacy policy what personal information the company collects?	**Assessor Responses**	**Percentage**
Yes	44	73%
No	16	27%
N/A: Company has no written privacy policy	4	N/A
Is it easy to determine from the privacy policy why the company collects the personal information?		
Yes	47	78%
No	13	22%
N/A: Company has no written privacy policy	4	N/A
Is it easy to determine from the privacy policy how the company uses consumers' personal information?		
Yes	42	70%
No	18	30%
N/A: Company has no written privacy policy	4	N/A
Is it easy to determine from the privacy policy to whom the company discloses consumers' personal information?		
Yes	33	55%
No	27	45%
N/A: Company has no written privacy policy	4	N/A

It is important to note that all Assessors who participated in this study are highly educated law students. According to Statistics Canada's 2001 Census, only 25% of the adult population in Canada has some university education. In contrast, 45% have only elementary to secondary school level education. It is therefore likely that many more policies would be rated as difficult to understand if Assessors were drawn from a sample of ordinary consumers.

Completeness of Privacy Policies

Principle 4.8.2 stipulates that the information made available by companies regarding their information management practices shall include:

> *(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;*
>
> *(b) the means of gaining access to personal information held by the organization;*
>
> *(c) a description of the type of personal information held by the organization, including a general account of its use;*
>
> *(d) a copy of any brochures and other information that explain the organization's policies, standards, or codes; and*
>
> *(e) what personal information is made available to related organizations (e.g., subsidiaries).*

Assessors reviewed each company's privacy policy to test whether it included these requirements (other than item (d)). The results show that many companies' privacy policies are deficient.

Over one quarter of the policies reviewed (30%) failed to provide contact information for a privacy officer. 50% failed to provide adequate instructions on how to access one's information, and 38% failed to even address the issue. Over one quarter (27%) of the policies reviewed failed to describe the types of information about consumers that they hold, and 18% failed to describe what the company does with that information. Almost half of our sample of companies (47%) failed to describe the types of personal information they share with other organizations. Even ten (34%) of the 29 companies who admit in their privacy policies to sharing customer information with other organizations (see Table 4), did not describe the type of information they share with other companies.

Table 15: Compliance with Principle 4.8.2

Does the privacy policy provide contact information for the person accountable for the organization's privacy policies and practices?	**Assessor Responses**	**Percentage**
Yes	42	70%
No	18	30%
N/A: Company has no written privacy policy	4	N/A
Does the privacy policy specifically describe how consumers can get access to their personal information held by the company?		
Yes: Privacy policy clearly states how consumers can access their personal information	30	50%
Somewhat: Privacy policy discusses the right to access one's personal information but does not make it clear how or where to send access requests	7	12%
No: Privacy policy does not address this issue	23	38%
N/A: Company has no written privacy policy	4	N/A

Table 15 : Compliance with Principle 4.8.2 Cont'd

Does the privacy policy describe the type of information the company holds about consumers?		
Yes: Privacy policy clearly describes the type of consumer information the company holds	44	73%
No: Privacy policy does not specify the type of consumer information it holds	16	27%
N/A: Company has no written privacy policy	4	N/A
Does the privacy policy describe what the company does with personal consumer information?		
Yes	49	82%
No	11	18%
N/A: Company has no written privacy policy	4	N/A
Does the privacy policy describe what consumer information the company shares with other organizations including affiliates?		
Yes: Privacy policy specifies the types of personal information the company shares with other organizations	9	15%
Somewhat: Privacy policy gives examples, but not a complete list, of personal information shared OR the company specifies types of information shared in some contexts but not in others	23	38%
No: Privacy policy does not indicate what types of personal information the company shares with other organizations	28	47%
N/A: Company has no written privacy policy	4	N/A

Openness About Disclosure Practices

Assessors also reviewed privacy policies to determine the extent to which companies that share consumer information with affiliates and third parties are open about whom they share the information with. Results show that 45% of privacy policies assessed were unclear, even generally, on whom the companies disclose information to (see Table 14). Moreover, of the 29 companies in the survey sample who claim in their privacy policies to share consumer information with affiliates or third parties for secondary marketing purposes (see Table 4), none provided a complete list of the companies with whom they share information.

Table 16: Openness About Disclosure Practices

Where the company shares customers' personal information with other companies for secondary purposes, does the company provide in the privacy policy the names of companies with whom they share customers' personal information?	**Assessor Responses**	**Percentage**
Yes: Company provides a complete list	0	0%
Yes: Company gives examples by providing the names of some of the companies with whom it shares personal information	4	14%
No	25	86%

FINDINGS FOR PRINCIPLE 4.3 – CONSENT

Key Findings

Not surprisingly, the vast majority of online retailers we surveyed (78%) rely on opt-out methods, at least in part, to obtain consumer consent for secondary uses and disclosures of their personal information. Only 8% use opt-in methods exclusively, and a surprising 14% do not bother to get consent through any means when customers register or order on their site, even though they admit to secondary uses or disclosures or are unclear on this point.

Under PIPEDA, consent must be informed. Yet, 17% of the privacy policies reviewed were unclear about whether the company uses consumer information for marketing purposes, and 18% were unclear about whether the company shares consumer information with other companies. A further 6% of companies did not have privacy policies at all. In 31% of the cases we reviewed, the companies provided no notice via the privacy policy or otherwise during the registration or ordering process.

Moreover, during the registration or ordering process, the majority of the 64 companies we assessed (53%) provided notice to customers only via a link to the privacy policy, requiring consumers to visit the privacy policy and read through it for an understanding of what the company does with their personal information. Of these, 56% failed to bring the link to the privacy policy to the customer's attention during the registration or ordering process.

We found a number of misleading privacy policies. In particular, of the 60 privacy policies assessed, 18% suggest that the company uses opt-in consent when in fact it relies on opt-out consent. This misleads consumers into thinking that their information will not be used for secondary purposes when in fact it will.

Twenty-nine companies (48% of our sample) admitted to sharing consumer information with other companies for purposes other than the transaction in question (another 11 (18%) were unclear). Yet, ten of these companies (34% of those that clearly share) did not offer consumers a choice regarding this practice during the registration or ordering process.

The methods used by many online retailers to obtain consent from consumers do not meet the requirements for valid consent.

- Of those companies relying on opt-out consent, 50% did so merely via a link to an often lengthy privacy policy as part of the registration or ordering process. In these cases, the majority (52%) failed to bring the link to the privacy policy to the customer's attention.
- Of those companies that included an opt-out in their privacy policy, 60% buried it inconspicuously in the often lengthy policy.
- Ten companies in our sample offered fewer opt-out options during the registration or ordering process than via their privacy policies, without any indication to consumers that additional opt-out options were available via the privacy policy. This misleading practice was exacerbated by the fact that none of these companies bothered to bring their privacy policy to the attention of consumers during the registration or ordering process.
- Of those companies relying on opt-out consent, 50% did not offer an immediate opt-out option as part of the transaction; rather, consumers have to consent against their will initially and then take additional steps to opt-out.

In seven cases (11%), the retailer clearly required consent to a secondary purpose in order for the consumer to transact. In none of these cases did the consumer receive any value in exchange for such consent. In an additional 18 cases, Assessors were not sure whether consent to a secondary use or disclosure was mandatory, due to lack of clarity in the privacy policy or an absence of a written privacy policy. Thus, potentially 39% of companies we assessed are violating PIPEDA's "refusal to deal" section.

Knowledge and Consent

Principle 4.3 requires 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 further requires that:

> *To make the consent meaningful, the purposes [for which the information will be used] must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.*

Adequacy of Notice

CIPPIC tested the informed consent principle in part by asking Assessors to identify whether, based on a reading of the companies' privacy policies, they understood the purposes for which companies use personal information. Without a clear and complete explanation of what the company does with consumers' information, companies cannot be said to be obtaining meaningful consent.

Of the 60 privacy policies reviewed, Assessors indicated that in 22% of cases, it was difficult to ascertain from the privacy policy why the company collects consumers' personal information and in 30% of cases it was difficult to determine how the company uses consumers' personal information. In a surprising 18% of cases, Assessors reported that the privacy policy does not specify at all what the company does with personal information (see Tables 14 and 15). Depending on how the company obtains consent, this suggests that consumers may not even be able to provide informed consent in some cases.

Methods of Notifying Consumers

Assessors therefore also looked at companies' privacy policies and online ordering practices to determine how companies obtain informed consent from consumers for secondary uses of their personal information. Assessors looked at companies' practices both during the registration process (in cases where companies require customers to register prior to placing an order) and the ordering process.

Of the 64 companies in the survey sample, 34 (53%) provide notice to customers only via a link to the privacy policy, requiring consumers to visit the privacy policy and read through it for an understanding of what the company does with their personal information. Of these cases, 56% of companies fail to bring the link to the privacy policy to the customer's attention during the registration or ordering process. In 31% of cases, the companies provide no notice via the privacy policy or otherwise during the registration or ordering process. Hence, it is likely that many customers are unaware of the uses and disclosures of their personal information to which they are ostensibly agreeing.

Table 17: Notice Methods

Methods of notifying customers of secondary uses and disclosures of consumer information during registration/ordering	Number of Companies	Percentage
Via link to privacy policy; link not brought to customer's attention	19	30%
Via link to privacy policy; link brought to customer's attention	12	19%
Customer is required to review the privacy policy as part of the registration/ordering process	3	4%
Notice included in the registration/ordering process	10	16%
No notice during the registration/ordering process	20	31%

Form of Consent

According to Principle 4.3.4:

> *The form of consent sought by the organization may vary, depending upon the circumstances and the type of information.*

While opt-in consent is the strongest form of consent and is thus preferable from a privacy perspective, the Privacy Commissioner has approved the use of opt-out consent for secondary marketing purposes where the following requirements are met[5]:

- The personal information is demonstrably non-sensitive in nature and context.
- The information-sharing situation is limited and well-defined as to the nature of the personal information to be used or disclosed and the extent of the intended use or disclosure.
- The organization's purposes are limited and well-defined, and stated in a clear and understandable manner.
- As a general rule, organizations should obtain consent for the use or disclosure at the time of collection.
- The organization must establish a convenient procedure for opting out of, or withdrawing consent to, secondary purposes. The opt-out should take effect immediately and prior to any use or disclosure of personal information for the proposed new purposes.

Of the 64 companies in the survey sample, the vast majority (78 percent) use an opt-out consent method to obtain consent from customers for at least some secondary uses of their personal information during the registration or ordering process. Only five (8%) use opt-in consent exclusively, while a surprising nine companies (14%) do not employ either opt-in or opt-out consent during the registration or ordering process.

Of the 78% of companies that use opt-out consent, 50% do so merely via a link to the privacy policy, requiring that consumers access the privacy policy and read through it to understand how they can opt-out of unnecessary uses of their personal information. In these cases, the majority (52%) fail to bring the link to the privacy policy to the customer's attention. Once again, it is therefore likely that many customers are unaware of the uses and disclosures of their personal information to which they are ostensibly agreeing.

Table 18: Consent Practices

During the registration/ordering process, how does the company obtain consumers' consent for secondary uses and disclosures of their information?	Assessor Responses	Percentage
Opt-out (exclusively)	45	70%
Opt-out and opt-in	5	8%
Opt-in (exclusively)	5	8%
No opt-out or opt-in option during registration/ordering	9	14%

[5] Taken from the Office of the Privacy Commissioner of Canada Fact Sheet: *Determining the appropriate form of consent under the* Personal Information Protection and Electronic Documents Act, online: <http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp>

Table 19: Opt-out During Registration/Ordering

During the registration/ordering process, how does the company bring the opportunity to opt-out to the consumer's attention?	Assessor Responses	Percentage
Via link to privacy policy on registration/ordering page; link not brought to the consumer's attention	13	26%
Via link to privacy policy on registration/ordering page; link brought to the consumer's attention	7	14%
Consumer is required to review or agree to the linked privacy policy as part of the registration/ordering process	5	10%
Opt-out forms part of the registration/ordering process	25	50%

Conspicuousness of Opt-out Option in Privacy Policy

Assessors found that, in the 47 cases where companies provide an opt-out option in their privacy policies, the majority of those opt-out options (60%) were inconspicuously buried in the privacy policy.

Table 20: Conspicuousness of Opt-out in Privacy Policy

Is the opt-out option in the privacy policy conspicuous?	Assessor Responses	Percentage
Yes	19	40%
No	28	60%

Timeliness of Opt-out

In addition, Assessors reported that of the 50 companies who offer opt-out consent during the registration or ordering process, 50% allow consumers to opt-out only after agreeing to allow secondary uses or disclosures. In such cases, consumers must email, telephone, or mail a request to the company to be removed from the marketing list or to otherwise restrict secondary uses and disclosures. Such extra efforts no doubt increase the likelihood that consent will be assumed incorrectly.

Table 21: Timeliness of Opt-out

Does the company provide an immediate opt-out method for the consumer?	Assessor Responses	Percentage
Yes: Consumer can select the opt-out option before or during registration/ordering	25	50%
No: Consumer can only opt-out after agreeing to allow secondary uses or disclosures	25	50%
N/A: Company doesn't provide opt-out at all but uses opt-in consent only during registration/ordering	5	N/A
N/A: Company doesn't provide any opt-out method during registration/ordering	9	N/A

Misleading Policies and Practices

In the 50% of cases where companies do provide a mechanism for customers to actively opt-out during the registration or ordering process, Assessors noted a number of discrepancies between what consumers can opt-out of during the registration or ordering process and what consumers can opt-out of via the company's privacy policy.

In the 11 cases where such discrepancies were noted, all but one concerned cases where the opt-out during registration or ordering did not provide all of the opt-out options that were available in the privacy policy. Yet in these cases, the privacy policy was not brought to the consumer's attention. This finding suggests that customers of these online retailers may be misled into assuming that they have exhausted the full range of opt-out options during the registration or ordering process, when in fact, if they visited the policy, they would discover they had more opt-out options.

Table 22: Opt-out Discrepancies

Are there any discrepancies between what you can opt-out of during the registration/ordering process and what you can opt-out of via the privacy policy?	**Assessor Responses**	**Percentage**
Yes	11	26%
No	31	74%
N/A: Can't opt-out via privacy policy, only during registration/ordering	8	N/A
N/A: Can opt-out via privacy policy, but only opt-in during registration/ordering	4	N/A
N/A: Can't opt-out via privacy policy, only opt-in during registration/ordering	1	N/A
N/A: Can't opt-out via privacy policy or registration/ordering process, nor can you opt-in during registration/ordering	7	N/A
N/A: Can opt-out via privacy policy, but not during registration/ordering	2	N/A
What is the nature of the discrepancy?		
Opt-out during registration/ordering process does not provide all of the opt-out options available in the privacy policy	10	91%
Opt-out during registration/ordering process allows consumers more opt-out options than available in the privacy policy	1	9%

Disturbingly, Assessors also found that a number of companies in the survey sample purport to use opt-in consent when they do not in fact do so. Of the 60 companies whose privacy policies were available for assessment, 14 (23%) suggest in their privacy policies that they use opt-in consent for secondary uses of consumer information. However, only three companies that claim to use opt-in consent actually use opt-in consent during the registration or ordering process. The remaining 11 companies, (18%) are misleading consumers into believing that their personal information will not be used for secondary purposes when in fact it may be so used.

Table 23: Opt-in Consent

According to the privacy policy, does the company engage in certain secondary uses or disclosures only with positive opt-in consent of the consumer?	**Assessor Responses**	**Percentage**
Yes (accurate)	3	5%
Yes (inaccurate)	11	18%
No	46	77%
N/A: Company has no written privacy policy	4	N/A

Requiring Consent as a Term of Service

According to Principle 4.3.3, organizations 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 fulfill the explicitly specified, and legitimate purposes.*

Assessors noted seven cases in which companies require consumers to agree to secondary uses or disclosures in order to get the product or services. In none of these cases was the consumer given something of value in exchange for the consent. In 18 additional cases, Assessors were unable to determine whether the company required such consent as a condition of purchase.

Table 24: Requiring Customers to Agree to Secondary Uses of Personal Information

Does the company require that consumers agree to secondary uses or disclosures in order to get the product or service?	Assessor Response	Percentage
Yes	7	11%
No	39	61%
Unclear	18	28%

PART II: COMPLIANCE WITH INDIVIDUAL ACCESS

Key Findings

A large proportion of companies are failing to comply with the PIPEDA requirement to inform individuals of the existence, use and disclosure of their personal information upon request, and to give individuals access to that information.

One-third (35%) of the companies we tested did not respond at all to access requests.

Of the companies that did respond,

- 42% failed to provide details about the Requestor's personal information they had on file;
- 37% provided no account or an inadequate account of how they use the personal information; and
- 58% did not give a list of companies to whom they have or may have disclosed personal information about the Requestor;

despite being specifically asked for this information by the Requestor.

According to Principle 4.9:

> *Upon request, and individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information.*

Despite this requirement, 35% of the 72 companies to whom access requests were sent failed to respond at all.

Time Requirements

Pursuant to Principle 4.9.4:

> *An organization shall respond to an individual's [access] request within a reasonable time…*

And section 8(3):

> *An organization shall respond to a [access] request with due diligence and in any case not later than thirty days after receipt of the request.*

Requesters tested compliance with PIPEDA's time requirements by recording the dates they sent their access requests and the dates they received the company's response to their requests, allowing five business days for mail delivery. Most companies that responded did so within the 30 day time limit.

Table 25: Company Response Times

Response Time	Companies	Percentage
No response	25	35%
Within 30 days	41	57%
Within 45 days	4	5%
Within 60 days	2	3%

Access to Personal Information

As noted above, PIPEDA requires companies to give individuals access to their personal information held by the company.

Requesters asked companies to provide them with a copy of all the specific information about the Requester that the company contains in their files.

Of the 43 companies that both responded to the Requesters' requests and claimed to have information about the Requester, a significant minority (42%) did not provide Requesters with copies of specific information about them that the company had in its files.

Table 26: Provision of Customer Information

Did the company give you a copy of all specific information about you that they claim to have in their files?	Requester Response	Percentage
Yes	25	58%
No	18	42%
No: Company claimed not to have any information about the Requester	4	N/A

Account of Use

Principle 4.9.1 requires that:

> *In addition, the organization shall provide an account of the use that has been made or is being made of this information...*

Requesters tested this principle by asking companies to provide them with a full account of the uses to which the company had made or was planning to make of their personal information.

Of the 43 companies that both responded to the Requesters' requests and claimed to have information about the Requester, 37% of companies failed to provide a full account of how they use the individual's personal information.

Table 27: Account of Use

Did the company give you a full account of how they use your information?	Requester Responses	Percentage
Yes	27	63%
No	16	37%
No: Company claimed not to have any information about the Requester	4	N/A

Disclosure to Third Parties

Principle 4.9.1 requires that:

> *In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.*

Further, Principle 4.9.3 states:

> *In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.*

Requesters asked companies to provide them with a list of all companies with whom they had (or may have) shared the Requester's information, or to whom they may have disclosed the information if they could not identify with certainty the specific companies to whom they had disclosed the information.

Of the 33 companies that responded to requests, do not deny sharing information with third parties and admit to holding information about the Requestor, the majority (58%) did not comply with this requirement.

Table 28: Disclosure of Customer Information

Did the company give you a list of companies to which they have disclosed or may have disclosed your information?	Requester Responses	Percentage
Yes	14	42%
No	19	58%
No: Company claimed it does not share information with third parties	10	N/A
No: Company claimed not to have any information about the Requester	4	N/A

Overall Compliance with Principle 4.9

Overall, only a disappointing 21% of the 72 companies that received access to information requests complied fully with the Individual Access Principle of PIPEDA, i.e., responded within 30 days and gave a full account of use, a copy of all information they had about the Requester, and a full account of companies to whom they have or may have disclosed Requester's information.

Authentication

Although the study did not specifically set out to test whether companies in the survey sample had security measures in place to ensure that they provided personal information only to the rightful owner of that information, the study did gather some interesting results in this regard.

Requesters recorded whether the companies they contacted for access requests asked them to supply additional information verifying their identity. Of the 47 companies that responded to individual access requests, only 17% asked for some kind of authentication from the Requester before proceeding with the access request and supplying the Requester with personal information. While no firm conclusions can be made on the basis of these results, they suggest that at least some companies are failing to take appropriate precautions before releasing personal data to individuals.

Table 29: Authentication

Did the company request authentication prior to responding to the access request?	Requester Responses	Percentage
Yes	8	17%
No	39	83%
N/A: No response to access request	25	N/A

CONCLUSIONS

RETAILER COMPLIANCE WITH PIPEDA

The results of our compliance assessment of 64 online retailers under PIPEDA's Openness, Accountability, and Consent requirements, and of 72 online and offline retailers under PIPEDA's Individual Access requirements, indicate widespread non-compliance in all four areas.

While almost all companies we assessed had a privacy policy and were thus aware of the need to respect customer privacy, many failed to fulfill even basic statutory requirements such as providing contact information for their privacy officers, clearly stating what they do with consumer information, and responding to access to information requests. A significant proportion of the policies we examined were unclear on key points such as whether or not consumer information is shared with other companies. Many failed to provide a clear and conspicuous method for consumers to opt-out of unnecessary uses and disclosures of their personal information, often relying on a clause buried deep in a lengthy privacy policy that consumers are unlikely to review.

A number of policies we examined were misleading, suggesting for example that no secondary use or sharing of personal information would take place without the consumer's explicit consent, but then assuming such consent unless the consumer exercised an often inconspicuous or incomplete opt-out.

COMMON PITFALLS OF PRIVACY POLICIES

Incomplete Information

Most of the privacy policies reviewed in this study failed to provide at least some of the basic information on the company's data management practices as required under PIPEDA. A surprising proportion (10%) consisted of no more than two paragraphs, leaving consumers with almost no information about the company's information management practices. For example, one company's privacy policy merely stated: "We do not make your name or personal information available to any third party. All information collected by us is used to provide you with the highest level of convenience and service". This policy fails to inform consumers about the kind of information the company collects, how it is used by the company, how unnecessary uses can be stopped, how an individual can access their information, and who in the company is responsible for handling privacy inquiries.

Hidden Consents

Many of the policies we reviewed failed to properly notify and obtain consent from consumers to secondary uses or disclosures of their personal information. Frequently, notice of such uses and disclosures, as well as of how the consumer can opt-out of such uses and disclosures, was hidden in an often lengthy policy and was not at any time brought to the consumer's attention.

Regardless of how long a policy is, it should be easy for a person with limited education to quickly determine:

a) how and for what purposes their personal information is used internally by the company;

b) whether their personal information may be disclosed for secondary purposes and if so, to whom for what purposes; and

c) how the person can stop the use and disclosure of their information for secondary purposes.

Misleading Reassurances

Many privacy policies we reviewed open with statements designed to reassure consumers of the company's commitment to protecting consumer privacy, particularly with regards to the manner in which the company discloses consumer information. Such statements are fine as long as they are

not followed by significant qualifications that essentially gut them of meaning. In a disturbing number of cases we reviewed, however, companies made reassuring statements at the beginning of their privacy policies that were later contradicted in the privacy policy.

In one such instance, the privacy policy states up-front that the company does not: "sell or rent our customers' personal information to third parties". However, several paragraphs later in the privacy policy, the company admits to sharing consumer information with other companies for secondary marketing purposes. In two other cases, companies claim at the beginning of their privacy policies that they won't share consumer information with other companies, however, the companies later note that they share consumer information for secondary purposes with "affiliates" and "marketing partners".

Another common approach that we encountered is an initial statement such as "We do not sell or share your information without your consent", implying that the company will actively obtain consent from consumers prior to disclosing their information. However, these policies often later reveal, deep in the policy document, that the company is indeed assuming the consumer's consent to the sharing of their information.

In all of these cases, a customer reading the privacy policy may stop after reading the opening statement, feeling confident that their information will not be shared with anyone or will not be shared without their active consent. Meanwhile, the company is actually assuming the consumer's consent to share their information for secondary purposes.

Repetition of PIPEDA Principles

A common variation of the themes set out above is for companies to merely restate their legal requirements under PIPEDA rather than explaining their own data management practices in detail. Such restatements of the law fail to provide consumers with the information about company policies and practices to which they are entitled to under PIPEDA, and worse, can be misleading in the same way that the reassurances above are.

For example, one company provides the following statement under the heading "8. Openness": "Information about our policies and practices relating to the management of personal information will be made readily available to individuals." The policy does not however explain what consumer information the company collects, how the company uses consumer information and to whom, if anyone, consumer information is disclosed. This statement is essentially useless to anyone seeking information about the company's privacy practices. Moreover, by failing to actually provide the information about its practices, the company is clearly not complying with PIPEDA's Openness principle.

RECOMMENDATIONS FOR PIPEDA REFORM

The process of assessing retailer compliance with PIPEDA highlighted some problems with the legislation – problems that retailers must face in determining how to comply with PIPEDA, and that assessors face in determining how to measure compliance. These problems fall into two general categories: vague standards and drafting gaps. In the case of the former, more specific guidance is needed – if not in the statute, then in directions and implementation guidelines from the Privacy Commissioner. The latter can be corrected through amendments to the legislation.

More generally, the results of this study strongly suggest that Canadian data protection legislation provides inadequate incentive for companies to give consumers meaningful control over their personal information, and to be open about their data management practices.

VAGUE STANDARDS

"Unreasonable effort"; "Generally understandable"

Principle 4.8.1 mandates that individuals be able to acquire information about an organization's policies and practices without "unreasonable effort" and that organizations supply information about their policies and practices in a form that is "generally understandable". PIPEDA does not define these broad terms nor does it set out any minimum standards for organizations to follow in order to comply with these requirements. What constitutes "unreasonable effort" and "general understandability" will vary from person to person, depending on their level of education, literacy, patience, and other factors. Assessors, as well as companies, must make subjective judgments on these questions. It would be helpful to have some objective standards to apply to this determination.

Opt-in vs. Opt-out Consent

Principle 4.3.4 allows for the form of consent sought by an organization to vary, but PIPEDA does not distinguish between express, implied, deemed, and opt-out consent, and provides no prerequisites or criteria for reliance on each type of consent. While the Privacy Commissioner has published guidelines for determining the appropriate form of consent,[6] our findings demonstrate that this is not sufficient: some organizations lack even a basic understanding of the differences between opt-in and opt-out consent, not to mention the appropriate use of opt-out methods.

DRAFTING GAPS

Notice: Criteria for Valid Notice

The "knowledge and consent" provision set out in Principle 4.3.2 combines two important concepts that warrant separate attention in the statute: notice and consent. As with consent, PIPEDA does not set out specific criteria for notice. We found a number of instances in which companies provide consumers with a clear and conspicuous opt-out during the ordering process, but no clear notice of the secondary uses and disclosures in which the company engages. The Commissioner's findings regarding the prerequisites for valid opt-out consent[7] are helpful in this regard, but would be more helpful set out in the statute and applied to notice as well as consent.

We also found a wide range of practices with respect to notice – from clauses hidden in privacy policies to notices that consumers must read and respond to in order to complete an order. While the former is clearly inadequate and the latter is clearly adequate, it is not clear from PIPEDA where the line should be drawn. Setting out a separate requirement for notice with specific criteria would no doubt help companies ensure that their notice meets statutory requirements.

Notice: Content

Principle 4.8.2(e) requires that organizations state what personal information is made available to related organizations, but strangely ignores disclosures to third parties. Based on the results of our study, most organizations share customer information with unrelated third parties. Many do not have affiliates. By limiting this explicit notice requirement to related organizations, PIPEDA suggests that explicit notice regarding disclosures to unaffiliated third parties is not required. In any case, the limited scope of this disclosure requirement makes no sense; organizations should be required to give consumers clear notice of all personal information disclosures they make to third parties.

We also found it odd that the list of required disclosures in Principle 4.8.2, as well as in response to access requests under Principle 4.9.1, does not include sources. Individuals should have the right to know from where an organization obtains information about them.

---

[6] "Determining the appropriate form of consent under the *Personal Information Protection and Electronic Documents Act*", <http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp>

[7] Ibid.

Refusal to Deal

Principle 4.3.3 prohibits the refusal to supply consumers with goods or services on the grounds that the consumer does not provide personal information "beyond that required to fulfill the explicitly specified and legitimate purposes". This clause has been widely interpreted in the commercial context as meaning "beyond that necessary to provide the product or service". It should be revised accordingly, for application in the commercial (as opposed to employment) context.

ENFORCEMENT REGIME

PIPEDA's enforcement regime was purposefully designed to be "light handed", on the theory that a strong stick was not necessary in order to encourage companies to comply with the Act. Our findings - that a large proportion of retailers are not complying even with some of the most basic requirements of the Act - suggest that this "light handed" approach has not been successful and that alternatives should be considered.

TOPICS FOR FURTHER RESEARCH

Comprehensibility/Readability

This study used University law students as assessors. Yet, only one-quarter of the Canadian adult population has any university education, while close to half have elementary or secondary school education only. Further testing of the readability and comprehensibility of online retailers' privacy policies using a group that is representative of the average consumer population would produce a more accurate picture of how well organizations are communicating their data practices to the public generally. We strongly recommend that such a study be undertaken.

Authentication

Although the study did not specifically set out to test whether companies in the Individual Access survey sample had security measures in place to ensure that they provided personal information only to the rightful owner of that information, the study did suggest some shortcomings in this regard. Further testing could be conducted to determine whether organizations are complying with PIPEDA's security provisions by taking appropriate precautions before releasing personal data to individuals.

Audits

This study assessed companies' stated information management policies but did not test whether or how all of the policies we reviewed are actually put into practice. Such testing requires "mystery shopping" and/or on-site audits, which were beyond the scope of this study. The results of a mystery shopping exercise and/or on-site audits could be compared with companies' stated policies for a more comprehensive review of compliance with PIPEDA provisions.

Enforcement Regime

As noted above, the results of this study suggest that the current enforcement regime under PIPEDA is not working. Perhaps the most important issue for Parliament to consider during its five-year review of the legislation is the effectiveness of the existing "light-handed" approach to compliance, and alternative approaches to compliance and enforcement.