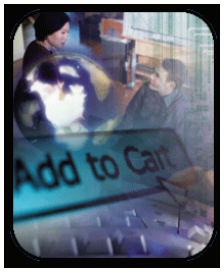
Incorporating Privacy into Marketing

and

Customer Relationship Management



A Joint Report of the

Information and Privacy Commissioner of Ontario

and the

Canadian Marketing Association

Information and Privacy Commissioner of Ontario

Canadian Marketing Association

May 2004

Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, and the Canadian Marketing Association gratefully acknowledge the contribution of the following individuals in the preparation of this paper: Colin Bhattacharjee, Project Analyst, Office of the Information and Privacy Commissioner of Ontario; and Mona Goldstein, President, The Goldstein Group.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario CANADA M4W 1A8
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Canadian Marketing Association
1 Concorde Gate, Suite 607
Don Mills, Ontario M3C 3N6
416-391-2362
Fax: 416-441-4062
Website: www.the-cma.org

Table of Contents

Introduction 1

CRM and Canadian Businesses 2

What is Privacy? 3

Private-Sector Privacy Legislation in Canada 4

What are Fair Information Practices? 5

Applying Fair Information Practices to CRM 6

FIP #1: Accountability 6

FIP #2: Identifying Purposes 7

FIP #3: Consent 8

FIP #4: Limiting Collection 9

FIP #5: Limiting Use, Disclosure, and Retention 10

FIP #6: Accuracy 10

FIP #7: Safeguards 11

FIP #8: Openness 12

FIP #9: Individual Access 12

FIP #10: Challenging Compliance 13

Conclusion 14

Notes 15

Introduction

With sales of more than $13.3 billion worldwide in 2003, Eastman Kodak's products and services reach millions of customers around the world.[1] As with many companies, Kodak engages in customer relationship management (CRM), a business strategy which focuses on developing a better understanding of the needs and preferences of customers so that a company can strengthen its relationships with its customers. But Kodak is going one step further – it is actively integrating privacy principles into its global CRM strategies, particularly with respect to marketing.

In 2001, Kodak's newly appointed chief privacy officer, Dale Skivington, approached the company's chief marketing officer and proposed that an internal privacy council be established that would take an internationally recognized set of privacy principles, known as fair information practices, and apply them to the marketing activities of all of Kodak's business units around the world, including those in Canada. After the council was established, it developed privacy guidelines for each type of marketing activity and the company began investing in CRM technology that complemented Kodak's emphasis on privacy.[2]

Businesses are increasingly recognizing that privacy can play a crucial role in the success of CRM initiatives. A 2002 study, by the U.S.-based Gartner research group, found that 40 per cent of companies were rethinking their CRM projects to include a greater emphasis on privacy.[3] In Canada, the extension of privacy legislation to the private sector is also influencing the implementation of CRM. As of January 1, 2004, the federal *Personal Information Protection and Electronic Documents Act* covers all private-sector organizations that collect, use or disclose personal information in the course of commercial activities, except in those provinces that have enacted substantially similar legislation.[4]

The challenge for businesses implementing CRM is to collect, use and disclose personal information in a manner that does not invade the privacy of their customers. Although CRM is used for a wide variety of purposes, the vast majority of Canadian companies use CRM for marketing purposes. In this paper, we will argue that building a privacy framework into CRM initiatives is not only a legal necessity in Canada but can play a pivotal role in maintaining customer trust and loyalty, which is the ultimate goal of CRM. In particular, we will outline some practical steps that businesses can take to integrate fair information practices into their CRM projects, particularly those that involve marketing.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Province of Ontario

John Gustavson
President and Chief Executive Officer
Canadian Marketing Association

CRM and Canadian Businesses

Although there is little agreement on how to define CRM, it generally covers a range of activities used by businesses to gain insight into customer needs and behaviours in order to strengthen their relationships with their customers. In its "pure" form, CRM allows businesses to better understand the individual needs and preferences of their key customer segments, and to serve different customers differently.[5] CRM encompasses strategies and technologies that are enabling companies to move from product-centric business models to ones that are customer-centric.

A CRM benchmark study, published by the Canadian Marketing Association (CMA) in 2002, found that 86 per cent of Canadian companies in nine sectors of the economy practised some form of CRM.[6] Although the study found that CRM is still developing in Canada, it noted that CRM expenditures were projected to top $800 million in 2003 and climb at a compound annual growth rate of 15 per cent.[7] In short, CRM is rapidly becoming entrenched as an established business practice in the Canadian marketplace.

What is Privacy?

In North America, the legal concept of privacy was first explored in an 1890 article in the *Harvard Law Review* by Professors Samuel Warren and Louis Brandeis who defined privacy as "the right to be let alone."[8] This definition of privacy has evolved over the last century to include at least two strands: the right of individuals to control their physical space (i.e., their body or home) and to control their personal information. The latter right is known as "informational privacy" or data protection.

Consequently, privacy includes the right of individuals to control the collection, use and disclosure of personal information about themselves. Personal information can be defined generally as identifiable information about an individual. In other words, it is information that serves to identify a person and could include his or her name, address, telephone number, date of birth, age, marital or family status, financial status, e-mail address, etc.

Private-Sector Privacy Legislation in Canada

The federal government enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA) to protect personal information that is collected, used and disclosed by private-sector organizations in the course of commercial activities. The legislation has come into effect on a staggered basis. On January 1, 2001, PIPEDA applied to federally-regulated businesses such as banks, railways, airlines and broadcasting companies. On January 1, 2004, the legislation further extended to provincially regulated businesses, unless a province had enacted substantially similar privacy legislation. Quebec has had private-sector privacy legislation in place since 1994.[9] British Columbia[10] and Alberta[11] brought in their own private-sector privacy legislation on January 1, 2004. However, businesses in other provinces, such as Ontario, are subject to PIPEDA.

What are Fair Information Practices?

Canada's privacy laws are based on fair information practices which are a set of common standards that balance an individual's right to privacy with an organization's legitimate need to collect, use and disclose personal information. In 1980, fair information practices were internationally codified in the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[12] In 1996, these standards were incorporated into the Canadian Standard Association's *Model Code for the Protection of Personal Information* (CSA Model Code).[13] The CSA Model Code, which is appended as a schedule to PIPEDA, includes the following 10 fair information practices:

- Accountability
- Identifying Purposes
- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Applying Fair Information Practices to CRM

CRM initiatives involve the collection, use and disclosure of personal information, particularly for marketing purposes. Since understanding customers is critical to building relationships, businesses implementing CRM may collect information about who their customers are, what they purchase, their satisfaction levels and their channel preferences. Individuals interact with businesses through a variety of channels – stores, call centers, websites, e-mail campaigns, telemarketing, direct mail campaigns and sales people in the field. Although only half of Canadian companies can currently integrate customer data across service channels,[14] the promise of CRM is that the more holistically a company can view information from disparate sources, the more it can tailor products and services to fulfill customers' wants, needs and preferences. As CRM sophistication increases, so does the need to implement appropriate safeguards for personal information and to abide by customers' privacy expectations.

To comply with the requirements of privacy legislation and to avoid alienating customers, businesses must find ways to incorporate fair information practices into CRM initiatives. However, since CRM includes a loosely defined range of activities that could change over time, incorporating fair information practices into CRM may not always be straightforward. Consequently, the actions taken to protect privacy may vary depending on the size of the business, the resources that are available for this purpose, the extent to which CRM has been incorporated into a company's business strategies, and the amount and sensitivity of the personal information that is collected, used and disclosed for the purposes of CRM.

FIP #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 following principles.

Many individuals within a business, such as sales, marketing or website staff, may be responsible for the day-to-day collection and processing of personal information for the purposes of CRM. However, a business must designate one or more specific individuals who are accountable for ensuring that the business complies with fair information practices and privacy legislation. In large companies, a chief privacy officer would typically play such a role. In medium and small companies, such a role could be fulfilled by a privacy officer or another designated staff person who is properly trained in privacy management.

As a best practice, the designated individual should be actively engaged in the design and implementation of CRM initiatives to ensure that fair information practices are taken into consideration. For example, as noted previously, Kodak's chief privacy officer approached the company's chief marketing officer shortly after she was appointed in 2001 and proposed that

an internal privacy council be established that would apply fair information practices to the marketing activities of all of Kodak's business units around the world.

It should also be noted that a business is responsible for personal information that is in its possession or custody, including information that has been transferred or outsourced to a third party for processing. Consequently, if a company hires an external CRM consultant to perform data analysis or a variable printing supplier to execute a mailing, it must ensure that these outside entities are contractually bound to provide a comparable level of privacy protection to this data.

Finally, a business must put into place policies and practices that give effect to the 10 fair information practices, including:

- implementing procedures to protect personal information;
- establishing procedures to receive and respond to complaints and inquiries from the public;
- training staff and communicating information to staff about the business's policies and practices; and
- developing information to explain the business's policies and procedures.

FIP #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.

According to the CMA's 2002 benchmark study on CRM, 90 per cent of companies collect basic "tombstone" information about their customers (e.g., name, address), purchase history, customer satisfaction information, and data on customer loyalty and retention.[15] More than 75 per cent of businesses also gather customers' opinions about their products, services and the overall industry.[16] Seventy per cent of companies collect demographic information about customers, such as their household income and age.[17]

Companies collect this information for a variety of CRM-related purposes. In general, it is collected for the purpose of better understanding and serving the needs and preferences of customers. However, there is a requirement that information must be gathered for specific, identified purposes. Companies must not solicit or collect information on an ad hoc basis or engage in "fishing expeditions" to accumulate personal information for some vague potential future use. Companies must articulate how they intend to use the information (e.g., for marketing purposes, for customer service, to administer a loyalty program, for credit verification, etc.) and collect only the information that is necessary for the identified purposes.

As a best practice, businesses should err on the side of transparency and be as open as possible when identifying the purposes for which they are collecting personal information from their customers.

Consumers may be informed about the purpose for which information is being collected in a variety of ways, depending on the communication channel. For example, if a consumer buys a product from a company's website and is asked to provide demographic information such as annual income and age, a privacy policy that identifies the purposes for the collection should be easily accessible on the website. In face-to-face or in-store interactions, it may be more practical to provide written policies or have staff trained so they can accurately answer questions from their customers.

When personal information that has been collected is to be used for a purpose that was not previously identified, the new purpose must be identified prior to its use. For instance, a hardware company may have initially collected the names and addresses of customers from filled-in ballot forms for the purpose of administering a contest. The company would have their customers' implied consent to use their information to inform them whether or not they had won the contest. However, if the company later wishes to use this contest information for other purposes, such a direct mail campaign for do-it-yourself products, it must obtain consent and provide an opportunity to decline from receiving marketing offers.

FIP #3: Consent

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

Business must seek permission from customers before collecting, using and disclosing their personal information for CRM-related purposes, such as presenting new marketing offers or renting a customer list to other companies. Customers must have the opportunity to provide informed consent, which means that they understand the nature and consequences of providing or withholding consent. In a multi-channel CRM environment, it is recognized that there are several appropriate methods of obtaining consent to conform to fair information practices and to build trust between companies and their customers. The law also takes a common sense approach to the sensitivity of the information being collected, used or disclosed.

Consent is commensurate with the sensitivity of the data. For less sensitive information, such as a customer's name, address or telephone number, it is appropriate for a company to seek opt-out consent. In other words, unless a customer opts out, a company would be allowed to use or disclose that individual's name, address or telephone number for the purpose of marketing new products or services to that customer. However, the opt-out consent must be clear, easy to understand and easy to execute. (A best practice may include offering a toll-free number to opt out.)

In some circumstances, where the marketing offer is intimately linked to an original transaction, companies may reasonably conclude that consent is implied and does not need to be specifically requested. For example, a magazine publisher would have a subscriber's implied consent to send out subscription renewals. However, the disclosure of personal information to a third party for marketing purposes can never be implied – it must be obtained by opt-out or opt-in consent.

If a company is collecting sensitive information from customers, such as their personal health information or financial information, it must not use or disclose this information for marketing purposes unless the individual has opted in (i.e., provided express, explicit consent). Beyond obviously sensitive information – medical, credit, financial, sexual orientation, etc. – companies should give serious consideration to how a consumer may regard other types of information prior to using it (e.g., certain magazine subscriptions).

Companies can allow customers to give consent in many ways – by mail, phone, online, in store or through any appropriate channels. Current best practices in Canada can be found in the privacy policies and practices of leading CRM companies. Examples include Hudson's Bay Company – hbc.com, Kodak Canada – kodak.ca, The Loyalty Group – airmiles.ca, RBC Financial Group – rbc.com and Reader's Digest – readersdigest.ca

Companies collecting personal information for CRM-related purposes must also give customers the opportunity to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The company must inform the customer of the implications of withdrawing. For example, if a customer is a member of a grocery chain's loyalty program but decides that she does not want her purchase histories recorded in a database, she should have the opportunity to withdraw her consent for this use of her personal information. However, the grocery chain should also inform her that by withdrawing consent, she may not receive the cost-saving benefits provided by the loyalty program.

FIP #4: Limiting Collection

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

Businesses must not collect personal information indiscriminately. Both the amount and the type of information that a business collects from a customer must be limited to that which is necessary to fulfill the identified purposes of a CRM project. For example, a company that manufacturers and sells snowboards may be interested in determining the average age of its customers so it can pinpoint which media are best suited to running its ads and promotions. Consequently, it may offer individuals who buy its snowboards the opportunity to fill out a "Win a Trip to British Columbia" contest ballot that asks for a customer's name, address, phone number, e-mail address and age. For this type of CRM initiative, it would not be necessary to collect further information, such as a customer's annual income or occupation, because this information would not be necessary for achieving the purpose of the project.

Companies must only collect personal information by fair and lawful means. In other words, they should not be deceptive or misleading about why they are collecting a customer's personal information. In the above example, the snowboard manufacturer should make it clear on the contest ballot form that it is collecting a contestant's age for marketing or media selection purposes.

FIP #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 the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.

Companies that collect personal information with consent for the purpose of developing a better understanding of the needs and preferences of their customers must ensure that this information is not used or disclosed for any secondary, unrelated purposes. For example, a bank's investment arm may have a CRM project that involves collecting and updating information about the annual income and assets of its customers for the purpose of marketing investment products to them. Unless the bank obtains consent from a customer, it should not use or disclose this information for other purposes that have nothing to do with that CRM project, such as determining eligibility for mortgages or insurance products offered by the bank. Personal information that is no longer required to fulfil the identified purposes of a CRM project should be destroyed, erased or aggregated, thereby rendering the data anonymous.

FIP #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.

The CMA's 2002 benchmark study on CRM notes that customer segments are valuable only to the extent to which they are current.[18] Consequently, personal information must be reviewed and updated on a regular basis to ensure that CRM databases reflect the present and not the past status of customers. Forty-two per cent of companies practising CRM update their customer segments on an annual basis, while another one-third do so on a quarterly or monthly basis, or even more frequently.[19]

Maintaining accurate, complete and up-to-date information about customers makes sense from both a business and privacy perspective. One aim of CRM is to enable businesses to better understand the individual needs and preferences of their key customer segments, and to serve different customers differently.[20] If a CRM database contains inaccurate or misleading information, this can have an adverse effect on a company's efforts to identify and market relevant products to its various customer groups and, conversely, may erode a customer's trust in a company.

Businesses may collect personal information about their customers through a variety of channels – stores, call centers, websites, e-mail campaigns, telemarketing, direct mail campaigns, or sales people in the field. A company that is implementing a CRM initiative that involves collecting or updating personal information should put policies and procedures in place to ensure that any information that is gathered is accurate, complete and up-to-date.

FIP #7: Safeguards

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

More than 90 per cent of Canadian companies use technology to support their CRM efforts.[21] For example, sales people in the field may collect and store personal information about customers in a laptop computer or personal digital assistant and transmit this information back to the office electronically. Similarly, a customer may provide personal information electronically while filling out a website survey that a company has set up as part of a CRM initiative.

Regardless of whether personal information is stored in paper or electronic format, companies practising CRM must put in place security safeguards (e.g., locked filing cabinets for paper records), that protect such information against loss, theft or unauthorized access. The nature of the safeguards will depend on the sensitivity of the information. Highly sensitive information, such as an individual's specific income, should be accorded a higher level of protection.

CRM databases are a lucrative target for identity thieves because they contain a wealth of information about customers. To minimize this risk, access to such databases should at the very least be password-controlled and limited to those employees who need such access to perform their job duties. Companies should also take special care when destroying or disposing of personal information from CRM databases to ensure that unauthorized parties cannot access or reconstruct the information.

Privacy-enhancing technologies such as encryption can also play an important role in protecting databases from being viewed by unauthorized individuals. Encryption is a mathematical process that changes data from plaintext (which can be read) to cyphertext (an unintelligible or scrambled form). In order to reconstruct the original data or decrypt it, an individual must have access to a decryption key. Ideally, personal information should be encrypted when it is stored in a CRM database or transmitted over the Internet as part of a CRM initiative.

FIP #8: Openness

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

The expanding scope of privacy legislation is making citizens increasingly aware and conscious of their privacy rights. According to a 2002 Harris Interactive survey, 83 per cent of American consumers would stop doing business with a company entirely if they heard or read that the company had misused customer information.[22] A Forrester Research survey of both Americans and Canadians found that almost 90 per cent of online consumers wanted the right to control how their personal information was used after it was collected.[23]

To enhance customer trust and loyalty, companies practising CRM should be open about their policies and practices with respect to the management of personal information. Customers should be able to easily acquire information about a company's privacy policies and procedures, and this information should be written in plain, simple language.

Again, best practices in privacy policies can be seen on the websites of the companies listed in FIP #3.

FIP #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.

CRM marketers know that accuracy of information and honest dealings are mission critical components of successful customer relationships. When asked, companies must share the personal information they hold about individual customers and amend any inaccurate data. They must also provide specifics about any third parties to which they have disclosed personal information, to the best of their ability.

A business must respond to a customer's access request within a reasonable time and at minimal or no cost to the individual. It must also provide the information in a form that is generally understandable. For example, if CRM software uses certain abbreviations or acronyms to record customer information, the company must provide an explanation of what these codes mean. However, companies are not required to reveal commercially proprietary information.

If a customer successfully demonstrates that the personal information held by the company in a CRM database is inaccurate or outdated, the company must correct the information as quickly as possible. If an individual is not satisfied that the company has properly corrected an error in his or her personal information, and the dispute cannot be resolved, the company must attach a statement of disagreement to the customer's record in the CRM database that reflects the customer's position.

FIP #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.

A company must put procedures into place for accepting and responding to complaints that customers may have about its data-handling practices. The chief privacy officer or other individuals who are accountable for ensuring that the business complies with privacy legislation should take the lead in investigating and resolving any complaints. If the investigation determines that a particular CRM practice is not in compliance with the applicable privacy law, the company must take appropriate measures to remedy the situation.

Conclusion

CRM is a firmly entrenched business practice in the Canadian and American marketplace. It allows companies to provide better service to consumers and to tailor products, services and marketing offers based on the knowledge of who their customers are. Leading CRM marketers recognize the importance of building privacy and customer preferences into the system, right from the outset.

Businesses should view privacy as a tool for ensuring that CRM initiatives succeed. This can be achieved by building fair information practices into CRM, with a particular focus on being open and transparent with customers. In short, privacy is good for CRM and can help companies to gain a competitive advantage in the marketplace by building strong customer relationships based on a foundation of trust.

Notes

1. Eastman Kodak Company, News Release, "Kodak Has 4th-Quarter Reported Net Income of 7 Cents Per Share," January 22, 2004, <www.kodak.com/US/en/corp/pressReleases/pr20040122-05.shtml>.

2. Telephone interview with Dale Skivington, March 1, 2004.

3. "Report: Companies Must Balance Privacy with CRM Programs," *DM Review*, January 2002, <www.dmreview.com/editorial/dmreview/print_action.cfm?articleId=4595>.

4. S.C. 2000, c. 5, <www.privcom.gc.ca/legislation/02_06_01_e.asp>.

   Please recognize that this document does not offer legal advice nor does it intend to provide an interpretation of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). It does provide best practices for your organization to consider in its administration of PIPEDA. Please consult your own legal advisors on steps your organization may need to take to ensure compliance with PIPEDA.

5. Canadian Marketing Association (CMA), "CRM Benchmarks: Canada 2002 Edition – A Roadmap for Improving Customer Relationships," p. 7. The CMA, the Carlson Marketing Group and The Loyalty Group jointly sponsored the study. Decima Research Inc. conducted the study in partnership with Deloitte Consulting. To order the study, go to: <https://www.the-cma.org/forms/crmbenchmarks_form1.html>.

6. Ibid., pp. 11, 17.

7. Ibid., p. 7.

8. <www.louisville.edu/library/law/brandeis/privacy.html>.

9. *An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. c. P-39.1*, <http://publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_39_1/P39_1_A.html>.

10. Bill 38, *Personal Information Protection Act*, 4th Sess., 37th Parl., British Columbia, 2003 (came into force on January 1, 2004), <www.legis.gov.bc.ca/37th4th/3rd_read/gov38-3.htm>.

11. *Personal Information Protection Act*, S.A. 2003, c. P-6.5, <www.qp.gov.ab.ca/documents/acts/p06p5.cfm?frm_isbn=0779725816>.

12. <www1.oecd.org/publications/e-book/9302011e.pdf>.

13. <www.csa.ca/standards/privacy/code/default.asp?language=english>.

14. Supra note 5, p. 51.

15. Ibid., p. 41.

16. Ibid.

17. Ibid.

18. Ibid., p. 43.

19. Ibid.

20. Ibid., p. 7.

21. Ibid., pp. 13, 57.

22. News Release, "First Major Post-9/11 Privacy Survey Finds Consumers Demanding Companies Do More To Protect Privacy; Public Wants Company Privacy Policies To Be Independently Verified," February 20, 2002, <www.harrisinteractive.com/news/allnewsbydate.asp?newsid=429>.

23. News Release, "Forrester Technographics Finds Online Consumers Fearful of Privacy Violations," October 27, 1999, <www.forrester.com/ER/Press/Release/0,1769,177,ff.html>.

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario CANADA M4W 1A8
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Canadian Marketing Association
1 Concorde Gate, Suite 607
Don Mills, Ontario M3C 3N6
416-391-2362
Fax: 416-441-4062
Website: www.the-cma.org