

Multi-Application Smart Cards: How to do a Privacy Assessment

**A Joint Project of
The Information and Privacy Commissioner/Ontario
and
The Advanced Card Technology Association of Canada**



**Information and Privacy
Commissioner/Ontario**



**Advanced Card
Technology Association
of Canada**

August 2000

The Advanced Card Technology Association of Canada and the Information and Privacy Commissioner/Ontario gratefully acknowledges the work of *Catherine Johnston, Keith Saunders (MAOSCO)* and the *Office of the Information and Privacy Commissioner/Ontario* in preparing this report.

Note: This paper is an update to the 1997 publication, *Smart, Optical and Other Advanced Cards: How to do a Privacy Assessment*.

This publication is also available on the IPC Web site.



**Information and Privacy
Commissioner/Ontario**
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: <http://www.ipc.on.ca>



**Advanced Card Technology
Association of Canada**
831 Miriam Road
Pickering, Ontario L1W 1X7
905-420-3520
Fax: 905-420-2729
Web site: www.actcda.com
Email: info@actcda.com

Table of Contents

Foreword	1
Chapter 1 — The Basics	2
What Is Privacy?	2
Why Is Privacy Important?	2
The Impact of Computer Technology on Privacy	3
What Is the Role of This Document?	5
Chapter 2 — Privacy Protection Principles	6
Recognition and Respect for Privacy	7
Openness	7
Purpose Specification	7
Collection Limitations	8
Notification	8
Use	8
Right of Access	8
Right of Correction	9
Accuracy	9
Disclosure	9
Retention and Disposal.....	9
Security	10
Aggregation	10
Accountability	10
Contractual Agreements	10
Anonymity and Pseudonymity	11
Chapter 3 — Privacy Assessment Checklist	12
Description of the Proposed System Based on Advanced Cards.....	12
Security of Multiple Sources of Information	13
Description of the Personal Information to be Collected.....	13
Purpose of the Collection	14
How is Notice of Collection Given and Informed Consent Obtained?	14
Method of Collection	15
Duration of the Collection of Personal Information	15
Accuracy	16
Method of Storage	16
Key Personnel.....	16
Description of Procedures for Access and Correction.....	17
Procedures for Complaints and Appeals of Denial of Access or Correction	17
Security	17

Chapter 4 — Privacy and Your Application	18
During the Design and Development of the Application	18
Rules for Multiple Application Systems	19
Chapter 5 — The Process of Implementing Privacy	20
Protection of Privacy as a Corporate Strategy	20
The Corporate Planning Phase	20
Documenting the Privacy Protection Policies and Procedures Phase	21
Maintaining the Privacy Protection Phase	21
Conclusion	22
Appendices	23
Appendix A — OECD Guidelines	25
Appendix B — Privacy Protection Assessment Checklist	27
Appendix C — Data Field Checklist	31
Glossary	32
Bibliography	34

Foreword

The Advanced Card Technology Association of Canada (ACT Canada) is a non-profit association that provides a voice for all advanced card and biometric technologies in Canada. Advanced cards use technologies with capabilities that surpass the currently used magnetic stripes you find on many of the cards you carry in your wallet. Smart, optical and capacitive cards are in use around the world and are now used in Canada. The technology allows more information to be stored and transported than do the existing mag stripes, which contain very little information. Each of the new technologies can be used for applications that may be of benefit to Canadians. These cards, and devices such as cell phones, Personal Digital Assistants, pagers and others, are emerging as personal information devices (PIDs). Applications using PIDs need to adhere to personal information protection standards. ACT Canada has worked with the Office of Information and Privacy Commissioner/Ontario to develop this privacy assessment so that application developers can build protection of privacy into advanced card technology and PID applications.

The Office of Information and Privacy Commissioner/Ontario (IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the Acts) to research and comment upon matters relating to the protection of privacy. In the fulfillment of that mandate, the IPC is concerned that all information technologies, if not properly managed, could represent a threat to the privacy of the residents of Ontario.

Together, the IPC and ACT Canada have produced this document to help companies and organizations understand and implement, in a practical way, the principles of privacy protection. Both organizations feel strongly that in order to successfully and economically implement privacy protection, it must be one of the basic design criteria in any technology application. By understanding and incorporating privacy protection throughout all the stages of development and implementation, organizations can produce applications that are both attractive to customers and sensitive to privacy concerns, thereby meeting their business need.

By collaborating on this document, we hope to provide you with a basic understanding of fair information practices, used in many countries to protect the informational privacy of individuals. We also wish to provide a process whereby you can incorporate privacy protection into your application design — the easiest and most cost-effective time to deal with it. Lastly, through the use of the two checklists developed, you will not only have ensured that you have thought through the various principles, but you will also have documented your protection of privacy design.

Good Privacy means Good Business!

Ann Cavoukian, Ph.D.,
Information and Privacy
Commissioner/Ontario

Catherine Johnston,
President & Chief Executive Officer,
Advanced Card Technology
Association of Canada

Chapter 1

The Basics

What Is Privacy?

Privacy is often confused with the more commonly understood concept of confidentiality. Confidentiality refers to the duties or obligations of individuals to safeguard the information they have been entrusted with.

Privacy has been described in various ways ranging simply from ‘the right to be left alone,’ to the interest that individuals have in sustaining a ‘personal space,’ free from interference by others.

Privacy has several dimensions. One is the protection of our personal data, also called informational privacy or data protection. Individuals do not want data about themselves automatically made available to other individuals or organizations without their consent, and that, even where data is held by another party, the individual must be able to exercise a substantial degree of control over that data and its use.

Why Is Privacy Important?

Think of your own privacy for a minute. Who knows what about you? If you begin with your wallet and the cards you carry, you start to realize that a lot of companies, governments and other organizations know, and likely have stored somewhere, your personal information. Now, let’s take that a step further. Are you sure that you know every organization or company that has your personal information in its possession? If a company that you gave information to sold it to another company, you might not know. In which case, you would find it very difficult to identify the new companies which now have your personal information, to check the completeness and correctness of that data, and correct any errors or omissions.

Your information belongs to you — maybe not the paper file it resides in or the disk it is stored on, but the information itself is truly yours. Therefore, you have a right to determine who has access to it, to authorize what it is used for, and to be provided with a mechanism to review the data and bring about any necessary corrections. Yet as you go about your everyday life, you are frequently asked to provide information about yourself to others. Joining a video or book club, using a preferred customer card, getting money from the bank; all these actions produce a set of electronic records which singly, and in combination, provide insight into you and your habits. Such information is a valuable commodity, which is regularly bought and sold, usually without your knowledge.

Now, let's look at this from a business perspective, rather than a personal perspective. Information is a fundamental commodity of today's business world. In today's information economy, the quality and integrity of information is of paramount importance. Customer service, in terms of identifying and meeting their needs and expectations, is one of the central tenets of today's business environment. Your customer is a source of valuable information that must be respected and protected. Today's customers are increasingly aware of and concerned about their privacy and the control of their information. When businesses become sensitive to this customer concern, their ability to successfully market their products and services will be greatly enhanced.

Consumer polls have consistently demonstrated that privacy protection is a significant concern of Canadian and international consumers. Surveys of Canadians consistently reveal a high degree of concern about privacy and a fear among consumers of losing control over the circulation and use of their personal information by companies. A 1998 poll done by Angus Reid concluded that Canadians overwhelmingly found it unacceptable for companies to sell, trade or share customer information with other companies. Similarly, Canadians believe that their personal information should be kept completely confidential except in certain circumstances. This desire for control over personal information is not unique to Canadians. A comprehensive survey conducted by Forrester Research in 1999 found that two-thirds of American Web consumers have serious concerns about privacy, while 80% want Web policies that prohibit the sale of their data to other organizations and 90% want control over their personal data. More recently, a survey conducted by Yankelovich Partners, released in August, 2000, found that 90% of consumers felt that the protection of personal privacy is the most important issue associated with e-commerce transactions. This concern for privacy is starting to affect business practices. Companies are increasingly recognizing that responding to their customers' desire to control the use of their personal information makes good business sense and can provide a competitive advantage in the marketplace.

The Impact of Computer Technology on Privacy

As we said earlier, technology allows information to move quickly and often invisibly. In the past, some comfort could be taken from the fact that your personal information was buried in paper files and would be very difficult for unauthorized parties to retrieve. Paper information was also held in physically separate locations, making it very difficult to collect information on different aspects of a person's life to allow a more detailed analysis to be performed. Today's databases, networks and the Internet, however, remove that procedural protection and physical barriers.

In mainframe computer applications, privacy was often a subset of security. Your salary information was available only to authorized people because the payroll application was designed to meet the security needs of the company. The same was true of human resources information. As we moved from mainframes to PC, we started to look at the computer, and therefore the security, differently. Information stored on our PC is often viewed as personal. It is our

correspondence, our spreadsheets and databases and basically the information we use to do our work. We started to view the data as being ours, as opposed to belonging to the company. Because we thought of it as “ours,” we often give it to co-workers if we feel they need it for their work. Another security weakness is that data on one’s PC is relatively easy to access. Just turning on someone’s PC may give you the ability to access his or her computer files, and today, hackers can break into networked computers from anywhere in the world.

Advanced cards¹ allow individuals to carry more information in their wallets than they did formerly. Smart cards are basically a PC on a credit card-size piece of plastic. Like PCs, they are capable of running multiple applications that can store data from multiple sources and perform computations on that data. Canadians use smart cards in telecommunications, transit, retail, banking, physical and data security and many other applications. Optical cards are also capable of storing massive amounts of data on a credit card sized piece of plastic. They work much in the same way as musical CDs and computer CD-ROMs. Canada’s Federal Government is currently testing this technology for frequent travelers. It may be used by authorized frequent travelers to clear customs by using a kiosk rather than being interviewed by a Canada Customs agent. Capacitive cards store tokens that can then be used in exchange for products or services. In several British Columbia communities, these cards are used by transit companies to allow commuters to prepay their travel and to easily board buses.

In each of these applications, there is personal information that should be protected, but that information is a part of the overall system, not just linked to the card or the application. In the case of electronic value, Canadians want to know who will have access to their purchasing information. With customs information, they want to know who will have access to their travel and declaration data. With transit, Canadians want to know who will know where and when they have traveled. And yet, this is coupled with the desire to have all the convenience and benefits offered by these cards.

With multi-application cards, there may be more than the card user and issuer involved. Third party suppliers or service providers may be used to manage card personalization, data management (including backup and restore functions), application loading and other functions. In this event, they must be bound by the same privacy protection rules and procedures as all other parties who have access to information related to the card. It is important to note that information may reside not only on the card, but also on other devices such as servers or even tape.

This document will help you, the developer, to design advanced card applications that build privacy protection into the application and surrounding components of the process.

¹ A glossary of advanced card and privacy terms can be found at the end of this paper.

What Is the Role of This Document?

This document will help you assess privacy protection in a systematic way. It will lead you through the overall process that surrounds your advanced card technology application. It will also help you to analyze the individual pieces of data that you may need to collect and use.

We need to return to systems designs that give thought to who is permitted access to each piece of data within an application and who is blocked from all access to an application. Who may see the data, add to it, change it or even delete it? How is the information protected when it is on a PC, or on a smart, optical or capacitive card? How do we treat the information when it is initially collected? Do we collect it on paper and then enter it into the application? If this is the case, how do we treat the forms after the data have been “entered”? How do we ensure that the data isn’t copied and given to others who were never intended to have access to it?

Protection of privacy must be viewed systematically at each stage from collection to destruction. The purpose of this document is to provide developers and marketers of applications using advanced card technologies with the background information and necessary tools to successfully meet the customer service goal of privacy protection. By understanding privacy principles and by following the process outlined in this document, you will be able to incorporate privacy protection into your applications, processes and procedures.

As information becomes more readily available through computers and the increasing use of the Internet, the public becomes more concerned about who has access to personal information. In some cases, Canadians are also worried that stored information about them may be incorrect and, if so, they would have no means of correcting it. While these concerns have always existed, even when information was written by hand on paper, computers have made the collection and distribution of information much easier and faster. This has in turn escalated most people’s concerns.

As smart, optical and capacitive card applications have been introduced into Canada, questions have been asked which are indicative of some of the misunderstanding as to how advanced cards work. The aim of this document is not to teach you about card technology, but rather how to build privacy protection into your applications².

Before we look at the system design elements, let’s first look at the principles involved in protecting privacy, often referred to as fair information practices.

² Should you wish to have a better understanding of advanced card technologies, you may contact the Advanced Card Technology Association of Canada at (905) 420-3520 or visit its Web site at www.actcda.com.

Chapter 2

Privacy Protection Principles

Many of the concerns expressed by consumers about privacy relate to the manner in which personal information is collected, used and disclosed. When organizations collect information without the knowledge or consent of the individual to whom the information relates, or use that information in ways that are unknown to the individual, or disclose the information without the consent of the individual, informational privacy is violated.

Concern about informational privacy in Europe in the early 1970s gave rise to the need for data protection. Data protection focuses on people's personal information and the ability to maintain some degree of control over its use and dissemination. What followed from the concern for data protection was the development of a set of practices commonly referred to as *Fair Information Practices*.

There have been several attempts to develop a complete and comprehensive set of fair information practices. One of the earliest efforts was made in 1980 by the Organization for Economic Co-operation and Development (OECD) in its *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Appendix A). The principles in that document have served as the model for privacy legislation such as the Ontario *Freedom of Information and Protection of Privacy Act* and for numerous privacy codes such as the Canadian Standards Association's *Model Code for the Protection of Personal Information*.³

More recent significant efforts to protect privacy have been the European Union's *Directive on the Protection of Personal Data with Regard to the Processing of Personal Data and on the Free Movement of such Data*, adopted on July 25, 1995, Québec's *Act Respecting the Protection of Personal Information in the Private Sector*, which sets out fair information practices for businesses operating in Québec, and the Canadian government's *Personal Information Protection and Electronic Documents Act*, formerly Bill C-6, which will initially apply to privacy in the federally regulated private sector and to cross-border commercial flows of information.

In its paper, *Privacy Protection Makes Good Business Sense*, the IPC presented a set of privacy practices that combined the use of personal information for business purposes with an individual's right to privacy protection. The practices that follow reflect these business practices, modified to fit the circumstances relating to advanced card technologies.

³ A copy of the *Model Code for the Protection of Personal Information* (document code CAN/CSA-Q830-96) can be obtained from the Canadian Standards Association, 178 Rexdale Boulevard, Etobicoke, Ontario, Canada, M9W 1R3

In regards to each of these principles, we would encourage those who design applications that use advanced card technologies and those who market them to commit to the following:

Recognition and Respect for Privacy

- recognize that your customers are the owners of their personal information, to be consulted in the development of policies or practices that could potentially impact their privacy
- adopt privacy protection practices and apply them when handling all customer personal information
- assess, prior to implementation, the impact on privacy of any proposed new policy, service or product
- adopt a policy of redress or restoration so that if any service alters the privacy *status quo*, you will provide a means to restore that privacy at no cost to the customer
- communicate your privacy protection policies and practices to your customers in a manner that enables customers to exercise their rights

Openness

- ensure that there is an openness about your policies and practices relating to your customers' personal information, and that the existence of any record-keeping systems containing your customers' personal information is not kept secret from them — descriptions of both policies and systems should be available for the customer to inspect
- develop and publicize a process for addressing and responding to any customer inquiry or complaint regarding the handling of personal information

Purpose Specification

- identify the purposes for which your customers' personal information is to be collected, used or routinely disclosed, before it is collected
- do not withdraw access to services or products if your customer subsequently refuses to permit the use of his or her personal information for a purpose not identified at the time of collection, including the exchange or sale of that information to a third party for marketing purposes

Collection Limitations

- only collect personal information about your customers that is necessary and relevant for the transaction(s) involved
- collect personal information about your customers directly from the individuals concerned, whenever reasonably possible
- collect customers' personal information with the knowledge and consent of the customers, except in very limited circumstances, and inform the customer of these circumstances at, or prior to, the time of collection

Notification

- notify your customers, at or before the time of collection, of:
 - the purposes for which the personal information is to be used or/and disclosed; and
 - the source(s) from which the personal information is to be collected, if not directly from the customer

Use

- only use personal information for the purposes identified to the customer at the time of collection unless the customer explicitly consents to a new use, or the activity is authorized by law

Right of Access

- establish a right for customers to have access to their personal information, subject to clear and limited exceptions (i.e., if such access would constitute an invasion of another person's privacy)
- provide customers with access to their personal information in a form understandable to them, without undue delay or expense
- if a customer is denied access, you should inform him or her of the reasons why and provide the customer with a fair opportunity to challenge the denial
- where an incorrect inference has been made from the analysis of multiple sources of information, the customer must have the right to correct the inference

Right of Correction

- establish a right for customers to challenge the accuracy of their personal information
- amend a customer's personal information if it is found to be inaccurate, incomplete, irrelevant or inappropriate
- make note in the customer's file of any discrepancies regarding the accuracy or completeness of his or her personal information
- take all reasonable measures to inform third parties who also use your customers' personal information, of corrections or changes that have been made

Accuracy

- take all reasonable and appropriate measures to ensure that the personal information you collect, use and disclose meets the highest possible standard of accuracy, completeness and timeliness

Disclosure

- obtain customers' consent prior to disclosure of their personal information, except where authorized by law or in exceptional circumstances. These limited, exceptional circumstances should be identified and customers informed of them at, or prior to, the time of collection
- obtain your customers' consent prior to renting, selling, trading or otherwise disclosing their personal information to a third party

Retention and Disposal

- retain personal information only for as long as it is relevant to the purposes for which it was collected, or as required by law
- dispose of personal information in a consistent and secure manner, or remove all references that would link the data to a specific identifiable person (thereby rendering it anonymous), once it has served its purpose

Security

- adopt appropriate and comprehensive measures to ensure the security of your customers' personal information against loss or unauthorized access, use, alteration, disclosure, or destruction
- where multiple sources of information are collected for different purposes, the security measures taken must ensure that one person cannot link the different sources of information together
- where multiple sources of information are held on the same physical device, the information must be separated such that the application controlling one set of information can not access the information controlled by another application

Aggregation

- where a company collects information on a customer for different purposes that information should remain separated unless the customer permits the information to be aggregated
- information from different sources should not be collated and analyzed to infer additional characteristics, behaviour, activities, or attributes of a customer without the prior permission of the customer

Accountability

- communicate your privacy policies and practices to all staff, and make your staff accountable for adherence to those policies and practices
- conduct periodic reviews of your privacy policies and practices to ensure that they are in keeping with your customers' expectations, as well as international developments

Contractual Agreements

- stipulate right in your contract:
 - the privacy protection measures to be adopted by business partners or third parties using your customers' personal information, and;
 - the purposes for which your customers' personal information may be used and disclosed by business partners or third parties

Anonymity and Psuedonymity

- reduce, to the greatest extent possible, the collection and retention of identifiable transactions. In other words, transactions in which the data in the record could be readily linked to an identifiable individual. This can be achieved through the use of either:

Anonymity — Ideally, there should be no personal identifiers involved in the transaction — you have “de-identified” it.

Psuedonymity — Where the functional or administrative needs of the application require some link between transactional data and identity, it is often possible to use pseudonymous techniques. These include such procedures as storage of partial identifiers by two or more organizations, both of whom must provide their portions of the transaction trail in order for the identity of the individual to be constructed; storing of an indirect identifier with the transactional data which serves as a pointer to the personal identifiers; and storing separately a cross-index between the indirect identifier and the individual’s true identity.

These are practices that are pertinent to your system as a whole. The following chapters contain checklists that should be completed for every new application or revision to an existing application. This will not only assist you in assessing whether your application adheres to fair information practices, but by completing it, you are also creating the documentation that will substantiate your application’s protection of privacy.

When designing for multi-application cards, it is important that all applications offer adequate privacy protection. It is equally important that all places that application data resides have equally adequate protection. This includes forms on which data is written or otherwise coded, databases and all other files.

Chapter 3

Privacy Assessment Checklist

The key to successfully implementing privacy protection into a system containing one, or more, applications is to consider it as one of the central design criteria. This will ensure that privacy protection is built into the system right from the start, thereby eliminating the difficult and expensive task of retrofitting privacy protection into an existing system.

The following components make up the privacy assessment checklist. Some apply during the development of an advanced card application while others are more applicable during the implementation stage and actual use of the application. Many of these components apply throughout all stages of development, implementation and usage. The checklist contains a few items that are only appropriate for a system that has, or will have, more than one application while most are specific for an individual application within the system.

The action you should take is printed in bold and italics. Background information has been included to assist you in preparing your answers. A checklist form that should prove helpful in completing this portion of the project may be found in Appendix B. It serves as a guide to the components needed to develop a privacy protection program, rather than a complete record of the program. Certain components may require the development of separate documents in order to completely describe and document the component. In those cases, the checklist will serve as a reference list for these documents. The checklist will also serve as an overview of the program that can be distributed to staff and customers to better inform them of the organization's commitment to privacy.

Description of the Proposed System Based on Advanced Cards

- *Describe the proposed multi-application system requiring the collection of multiple sources of personal information:*

Particular mention should be made of any common information that will either be held by the different applications in the system, or be used as a common customer identification mechanism within the system. The privacy implications of the applications sharing this data should be mentioned both from a positive and negative point of view. If the information can be aggregated then the inferences that can be drawn from the collection of information should be identified and noted.

- *Describe each proposed application requiring the collection of personal information:*

Particular mention should be made of the privacy implications of the application on both the positive and negative sides. The actual technology involved should be described as much as possible, in plain, non-technical language to make it accessible to your customers. While sufficient detail should be included to identify all the key components of the application, it should not reveal any information that would provide a competitive advantage. Important to include is whether the application may potentially affect the privacy of your customers and, if so, what methods will be introduced to minimize the intrusion and restore any lost degree of privacy.

Security of Multiple Sources of Information

- *Describe the security mechanisms that prevent information leaking from one application to another:*

The collation of information from multiple sources is always a concern within a multi-application system. This section should describe the security mechanisms that prevent one application from accessing the information being stored by another application when the information is stored within a common system or device. If a common identifier is used across more than one application then the security mechanisms that stop transactions using that identifier, from multiple applications, being collated should also be described. Where information is stored on a common system, the access control mechanisms and procedures used to prevent a single user of the system linking information from multiple applications together should be detailed.

Description of the Personal Information to be Collected

- *List and describe the personal information to be gathered:*

Personal information is information about an identifiable individual. For example; information related to a person's health, finances, entitlement to social benefits, travel plans or preferences, purchasing patterns, club memberships, or anything that links information to a specific, identifiable person. It includes, but is not limited to:

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, telephone number, fingerprints or blood type of the individual,
- (e) the personal opinions or views of the individual except where they relate to another individual,
- (f) the views or opinions of another individual about the individual, and;
- (g) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

The description of the personal information to be collected should also include such detail as:

- (a) does the information pertain to one individual or to a group of individuals;
- (b) what is the approximate number of records to be collected for each customer, and;
- (c) is any third party information involved.

Purpose of the Collection

- *Identify the purposes for the collection of personal information*

This helps the organization to clearly focus its information collection on only that which is necessary to fulfill the requirements of the application or the function it serves. Limiting the collection to only this necessary information simplifies the process as well as adhering to fair information practices. Consideration should be given to the use of pseudonymic techniques to alleviate the need to collect personal information.

How is Notice of Collection Given and Informed Consent Obtained?

- *Design, or attach, the notice to be authorized by the customer:*

Individuals must always be told when their personal information is being collected. Consent for the collection should be obtained before or at the time of collection. Sufficient information must be communicated about the purpose and process of the collection, retention, use and disclosure of the information for the individual to understand what is actually involved. It is also vital to highlight if the personal information will be shared with other organizations or linked to other databases.

Ideally, consent should be given expressly by the individual, but at times it can be reasonably implied by the fact that the individual has undertaken some action. For example, a consumer applying for a frequent flyer card could reasonably imply that all flights taken relating to that program will be noted and reported.

It is also key to ensure that the customer's consent is voluntary and informed. The customer must be knowledgeable enough to be able to weigh the advantages and disadvantages of providing the information in question. This ensures that consent is informed, and thus valid.

Method of Collection

- *Describe how information will be collected and, if appropriate, how it will be linked to previously collected information:*

Normally, personal information will and should be collected directly from the customer. If any personal information is collected indirectly, i.e., from some source other than the customer, it is important to justify the reasons for this to your customer and document the necessity for doing so.

It is important to identify any processes where personal information is linked or matched with other, previously collected information. Processes, which transfer the information from the point of collection to another point for use and storage, should also be identified.

Duration of the Collection of Personal Information

- *Identify the period of time over which the data will be collected:*

Many collections take place only at one time, but others do not. Some are limited in that there are start and finish dates to the collection, while others continue on an ongoing basis. Whenever possible, the collection should either be one time or limited in time since the continuous collection of information poses a threat to privacy. However, to fulfill the application's purpose or to ensure continued accuracy of the information, collection may at times have to be continuous.

Accuracy

- *Outline the steps to be taken to ensure that information is accurate at all stages of the application:*

Personal information must be verified by all appropriate means. Procedures within the application that ensure, as much as possible, the accuracy and timeliness of the personal information are key, not only from a business function perspective but also to reassure the customer — to provide her with the security that actions based on the information will be correct. Where information is gathered and then transferred (e.g., collected through the customer completing a handwritten form and then having the data keyed into the computer), how will accuracy be ensured? Also, how do you ensure accuracy when the electronic version of the data is copied, transferred or used in computations?

Method of Storage

- *List each method by which the personal information is stored, including the original collection form, computer files and copies, back up copies, on the advanced card, etc.:*

The format(s) in which the information is to be stored is also important. Some possible options are on the card, in segregated fields on the card, in dispersed databases, or in a centralized database. Safeguards to protect personal information within the application or its associated procedures are again key to the integrity of the data and to the customers' comfort level in allowing the use of their personal information. The level and sophistication of the safeguards should be in keeping with the customer's perception of the sensitivity of the stored information. Not to be forgotten are the original paper forms or entry transactions if they must be retained for record keeping purposes.

Key Personnel

- *List by name and title all personnel responsible for the privacy of this application:*

Certain key personnel associated with the application are crucial to identify. For the individual providing the personal information, these would include:

- (a) the overall custodian of the data who is responsible for the ongoing assurance of privacy protection;
- (b) the person responsible for answering questions or resolving customer complaints, and;
- (c) authorized users of the data along with the levels and/or types of access authorized for each type of user.

Description of Procedures for Access and Correction

- *Describe the process to be used by individuals to view and request changes to their data:*

Two components of privacy protection that are extremely important to consider before an application is developed are customer access and correction. Too often, customer access is not considered until the situation arises after implementation of the application. At that point, it may be too late. Certain decisions may have been made during the development phase which mean that access is either not possible, or prohibitively difficult or expensive.

Procedures for Complaints and Appeals of Denial of Access or Correction

- *Describe the procedure to be followed by an individual who wishes to lodge a complaint about his or her data or problems in accessing or correcting that data:*

Most important to the customer are procedures for his or her concerns to be addressed — customer service at its best. These concerns may take the form of complaints about how personal information is being treated. Individuals may also be concerned about a decision to deny them access to information that they feel is theirs, or to deny a request to change information that they feel is incorrect. Addressing these concerns in a timely fashion not only improves customer satisfaction but aids in ensuring the integrity of the information obtained — that it is not compromised by upset customers giving incomplete or incorrect information. Providing ways for individuals to *opt out* of the process or to *opt in* to only certain parts of the process is also of great benefit in achieving customer satisfaction.

Security

- *Describe the security measures that will apply to the information at all stages of its existence. See “Method of Storage”:*

Security issues are not new to anyone in the advanced card technology industry. They form a key component of any application. Adapting previously held notions of security in a privacy context is the challenge since security is only one component of privacy. Access controls and features to prevent unauthorized or unintentional disclosure of information can also be used to enhance privacy. Strong encryption algorithms exist to prevent unauthorized access and extraction of information. The level of security provided by various techniques must be commensurate with the potential harm caused by breaches of access and disclosure restrictions, and ideally, should be under the control of customer to select.

Chapter 4

Privacy and Your Application

Each time that you design a new application or modify an existing one, you should assess the impact of the application on privacy. It can become a natural part of your systems design process and will work well with your existing procedures. It starts by looking at each piece of data and determining who may access it and what they may do with that data element.

Each application on the card should follow this procedure. There may also be circumstances where common information on a card is accessed by more than one application. In that case, it is also important to complete the checklist for each instance. For example, if a customer's name and address are written on the card and are accessed by more than one application, you must determine the access rights of each application, treating the application as you would a person who accesses data.

During the Design and Development of the Application

Data Fields

You first start by identifying each piece of data that will reside on the computer or the card. You will find a checklist in Appendix B that you may copy and use during this phase of your application design. On the checklist, "communicate" refers to transmitting data over a communications port.

If your application was to gather frequent flyer points for a loyalty program, your checklist might include the following fields:

Data Field	Accessed By	Read	Add Data	Change	Delete	Copy	Print	Communicate
Card Owner Name	Card Owner	Y	N	N	N	N	N	N
	Issuer (Airline)	Y	Y	Y	Y	Y	Y	Y
	Travel Agent	Y	N	N	N	N	N	N
Frequent Flyer Number	Card Owner	Y	N	N	N	N	N	N
	Issuer (Airline)	Y	Y	Y	Y	Y	Y	Y
	Travel Agent	Y	N	N	N	N	Y	Y

Let's say the application is a health card. Your fields might include the following:

Data Field	Accessed By	Read	Add Data	Change	Delete	Copy	Print	Communicate
Patient Name	Patient	Y	N	N	N	N	N	N
	Issuer	Y	Y	Y	Y	Y	Y	Y
Drug Allergies	Doctor	Y	Y	N	N	Y	Y	Y
	Nurse	Y	N	N	N	N	Y	Y

It is important to identify each piece of data but equally important to identify it by location. That is to say that if you specify the access rights of the field on the central computer, you must do the same for that data field on the smart, optical or other advanced card, and also for any back up. Only then can you be assured that you have protected privacy relative to each piece of data.

When you have completed both this checklist as well as the privacy protection assessment checklist, you will have carefully and systematically planned for the protection of informational privacy for your application ... and you will also have documented it! Congratulations — you're way ahead now.

Rules for Multiple Application Systems

When data is accessed between applications, the above rules still apply.

Chapter 5

The Process of Implementing Privacy

While most of this document deals with the design and development of advanced card applications, let's take a moment to step back and look at protection of privacy as a corporate strategy.

Protection of Privacy as a Corporate Strategy

A key component of the successful development and implementation of privacy protection is the identification of a person who will be accountable for privacy protection within the organization. This designated individual may be your Chief Information Officer (CIO), or you may designate this as the responsibility of another person within your organization. The designated person may also be responsible for the management and co-ordination of the information resources policies and procedures of the organization. In either case, the person in this position must have sufficient authority to be heard by your executive management and senior staff. An increasing number of businesses have appointed a Chief Privacy Officer (CPO) to undertake this function. This person must have a good general knowledge of the business functions and processes of your organization as well as knowledge of information management techniques and tools. This person will become the advocate for privacy protection within your organization and for specific applications.

Depending on the size and structure of your organization, the CIO or other designated person may assemble a team of people from across the organization to first develop and then implement privacy protection. It is important that the team not be made up solely of staff with either technical or production responsibilities. Establishing broad policies and procedures needs input from all parts of the organization. Members of the team bring knowledge of the functions and processes of their part of the organization and take back both information about privacy protection and a commitment to making the principles work. Education of others will become an important part of their role.

The Corporate Planning Phase

As with any project, the planning phase is extremely important, and it is best to start with what is already known. Before privacy protection principles can be successfully integrated into an organization's policies and procedures, a thorough understanding of those policies and procedures is essential. Any organization that has information gathering, processing or distribution

functions will undoubtedly have information handling policies and procedures, which will likely include some of the components of privacy protection. It is vital at this point to identify the components in place and those that must be introduced. To do this successfully the team must know and understand privacy protection and particularly how it differs from such concepts as confidentiality and security.

Documenting the Privacy Protection Policies and Procedures Phase

Documentation is the most efficient and effective means of communicating the privacy protection of an organization to its customers and staff. It can also provide a clear and concise record of how the process of protecting information is to take place. The documentation should be in a form to make it readily available to those who need it. This may mean brochure format for the customer while the organization's staff is provided with a set of operational guidelines and procedures.

Maintaining the Privacy Protection Phase

- To fully benefit from all the work you have done in the previous phases, you need to provide ongoing education for existing staff and training for new staff
- You also need to periodically reinforce the importance of privacy to staff through such means as memos, internal newsletters, media-clipping services and internal case studies of both well-handled and poorly-handled privacy-related issues
- Periodic reviews and audits of established policies and procedures will give you an opportunity to acknowledge good practices and correct poor ones
- A periodic review of your policies and procedures will reinforce your corporate strategy
- Customer satisfaction surveys will show you where you are succeeding and where you are not, providing you with an opportunity to fine tune your procedures if necessary

The individual designated with responsibility for privacy protection should make a periodic report. A presentation to senior management on the status of the program should include the number of inquiries, the number of complaints, and the outcome of the complaints.

Conclusion

We hope that throughout this process you have thought about your own personal information and how important it is that no company misuse it. After all, we are all individuals and have some level of concern about our own information. At the same time that we may be the developers of one application, we are the customers of other applications. Just as we want to provide good customer service, we also want to receive good customer service. In the information economy, customer service is taking on a new look — that look is privacy.

Customers are increasingly demanding that companies respect their right to control their personal information and its use. By respecting this desire, companies will inspire consumer trust and confidence and ultimately, a reputation that will bring business dividends. Those companies that do not develop this trust relationship, or engage in business practices that misuse their customers' personal information, can expect to pay the price in terms of customer loyalty and satisfaction.

We all value our privacy in a general sense and we are becoming more sensitive about the protection of our information. The IPC and ACT Canada have jointly, through this paper, provided some tools to make privacy work for you. If you would like to receive more help in this area, both organizations would be happy to provide it.

Appendices

Appendix A

Organization for Economic Co-operation and Development

Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

Code of Fair Information Practices

Collection Limitation

Limited to the collection of personal data; data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification

The purposes for which personal data are collected should be specified not later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Purpose Specification Principle except: a) with the consent of the data subject, or b) by the authority of law.

Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller.

Individual Participation

An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him:
 - i) within a reasonable time;
 - ii) at a charge, if any, that is not excessive;
 - iii) in a reasonable manner; and
 - iv) in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraph (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability

A data controller should be accountable for complying with measures that give effect to the principles stated above.

Appendix B

Privacy Protection Assessment Checklist

Step	Details
<p>List Applications</p> <p><i>List all applications, including all common data fields</i></p> <p>e.g.: Driver's Licence Health Information Social Benefits Common data: name, address, birth date</p>	
<p><i>List data that can be inferred</i></p> <p>e.g.: card holder receives social benefits</p>	
<p>Description of the Proposed Application</p> <p><i>Describe the proposed application requiring the collection of personal information</i></p> <p>What are the important features? For example, what are the categories or groups of individuals you will be or are gathering information from and what classes or types of information are being gathered? What methods of collection, storage and transmission of the information are being used? How will the information be organized? For example, is the information for an individual retained together or stored separately by type such as identifying information in one location, transaction or functional information in another location?</p>	
<p>Description of the Personal Information to be Collected</p> <p><i>List and describe the personal information to be gathered:</i></p> <p>What type of personal information is to be collected? How is the information obtained (directly from the source or indirectly) and is any third party information involved? If the information is to be collected indirectly, the reasons why this is necessary should be clearly outlined. What differences, if any, are there for different categories or groups of individuals? Does the information pertain to one individual or to a group of individuals? What is the extent of the information to be collected, i.e., one record or several?</p>	

Step	Details
<p>Purpose of the Collection</p> <p><i>Identify the purposes for the collection of personal information:</i></p> <p>What are the reasons why the personal information is necessary and relevant to the application? Why must the personal information be collected in identifiable form? Why is personal information required as opposed to anonymous or pseudonymous information? What, if any, are the consequences of not collecting the personal information? Is the information required for functional or administrative purposes or both?</p>	
<p>How is Notice of Collection Given and Informed Consent Obtained?</p> <p><i>Design the notice to be authorized by the customer and attach.</i></p> <p>How is notice of the collection given? How is consent obtained? If it is not obtained directly from the individual, why is this necessary? What is the process by which the individual is informed and provides consent? Attach such documents as the application form used to seek consent, the response card sent in by the individual, a listing of the oral information provided when information is collected, etc. Is the information to be shared with other organizations or linked with their databases? If so, are fair information practices also in place there?</p>	
<p>Method of Collection</p> <p><i>Describe how information will be collected and, if appropriate, how it will be linked to previously collected information:</i></p> <p>What is the process of collection? How is the collected information transferred and stored? Is there any linking or matching with previously collected information and, if so, how is this accomplished? What controls are in place to ensure the validity of the information during the various steps of this process.</p>	

Step	Details
<p>Duration of the Collection of Personal Information</p> <p><i>Identify the period of time over which the data will be collected:</i></p> <p>Is the collection for this one time only, is it limited in duration or ongoing? Particularly important to note are the reasons why the collection is ongoing as this leads into issues of data integrity.</p>	<p>_____ one time</p> <p>_____ unlimited</p> <p>_____ limited</p> <p>Start Date: _____</p> <p>End Date: _____</p>
<p>Accuracy</p> <p><i>Outline the steps to be taken to ensure that information is accurate at all stages of the application:</i></p> <p>What steps will be taken to ensure the accuracy of the collected information both at the time of collection and over the course of time for information that may change? Is a verification process part of the overall process?</p>	
<p>Method of Storage</p> <p><i>List each method by which the personal information is stored, including the original collection form, computer files and copies, backup copies, on the advanced card, etc:</i></p> <p>What is the storage method and process for the advanced card application and associated components in the overall application?</p>	
<p>Key Personnel</p> <p><i>List by name and title all personnel responsible for the privacy of this application:</i></p> <p>Who is the Chief Information Officer of the organization, i.e., the person who serves as the focal point for the privacy protection process?</p> <p>Who are the people who have roles in the access and correction process?</p> <p>From the perspective of those inside the organization, it is useful to list persons who have key roles in the functions of collection, use, retention and disclosure of the information.</p>	<p>Chief Information Officer _____</p> <p>Other Key Personnel</p> <p>Name _____, Function _____</p> <p>Name _____, Function _____</p> <p>Name _____, Function _____</p> <p>Name _____, Function _____</p>

Step	Details
<p>Description of Procedures for Access and Correction</p> <p><i>Describe the process to be used by individuals to view and request changes to their data:</i></p> <p>What procedures are or will be put in place to permit customers to gain access to their personal information? What are the procedures for requesting correction of information? This might include reference to more detailed documents that describe the process at greater length. A document that is suitable for distribution to the customer is very useful, as is a document for internal use which outlines the steps of the access process and correction process for staff.</p>	
<p>Procedures for Complaints and Appeals of Denial of Access or Correction</p> <p><i>Describe the procedure to be followed by an individual who wishes to lodge a complaint about his or her data or problems in accessing or correcting that data:</i></p> <p>What procedures are in place for a customer to voice a complaint about how his or her personal information is being collected and used? What procedures exist if access to his or her information or correction of it has been denied? How are concerns resolved? What time frames exist for resolving them?</p>	
<p>Security</p> <p><i>Describe the security measures that will apply to the information at all stages of its existence. See “Method Of Storage”:</i></p> <p>What security measures are to be used to ensure the protection of personal information, restrict the possibility of unauthorized use and track authorized use. These measures should reflect the sensitivity of the data and should have the flexibility for customers to select security measures for their data which reflect their perception of the sensitivity of their data.</p>	

Glossary

Advanced Card	A card capable of carrying information. Uses technology more advanced than magnetic stripe. (See magnetic stripe, optical card, capacitive card.)
Anonymity	In this context, refers to the complete absence of identifiable data in a transaction.
Backup	An alternate or redundant device that replaces a primary device in order to maintain continued operation in the event of primary device failure.
Capacitive Card	A card where capacitive technology allows value to be stored as tokens. The technology does not allow the tokens to be reset, providing a measure of security.
Card	A rectangular paper or plastic medium used to carry information relating to its issuer and user.
Card Issuer	An individual or organization that issues identification cards.
Cardholder	Generally the person to whom a card is issued. For financial transactions cards it is usually the customer associated with the primary account number recorded on the card.
Card Personalization	The process of initializing a card with data that ties it uniquely to a given cardholder and/or account.
Encryption	The use of cryptographic algorithms to encode clear text data (e.g., PINs) to ensure that the clear text cannot be learned.
Personal Information Carrier	Any portable device capable of carrying information about individuals, e.g., smart cards, optical cards, cell phones, PDA's, etc.

- Pseudonymity** Pseudonymity refers to the use of an identifier for a party to a transaction, which is not, in the normal course of events, sufficient to associate the transaction with a particular individual. To explain in more detail, data can be indirectly associated with a person through such procedures as storage of partial identifiers by two or more organizations, both of whom must provide their portions of the transaction trail in order for the identity of the individual to be constructed; storing of an indirect identifier with the transaction data; and storing separately a cross-index between the indirect identifier and the individual's real identity.
- Magnetic Stripe Card** A card with one or more magnetic stripes.
- Optical Card** Also known as laser cards, because a low-intensity laser is used to burn holes of several microns in diameter into a reflective material exposing a substrata of lower reflectivity. The presence, or absence, or a burned hole represents bits. The areas of high and low reflectivity are read using a precision light source.
- Smart Card** A credit card sized piece of plastic with an embedded computer chip, i.e., capable of calculation.

Bibliography

Canadian Standards Association, *Model Code for the Protection of Personal Information*, 1996

Centre for Electronic Commerce for the Australian Commission for the Future, *Smart Cards and the Future of Your Money*, 1997

Clarke, Roger, *Privacy and Dataveillance, and Organizational Strategy*, 1996

Clarke, Roger, *What Do People Really Think? Mastercard's Survey of the Australian Public's Attitudes to Privacy*, 1997

Clarke, Roger, *When Do They Need to Know 'Whodunnit?' The Justification for Transaction Identification; The Scope of Transaction Anonymity and Psuedonymity*, 1995

Ekos Research Associates Inc., *Privacy Revealed - The Canadian Privacy Survey*, 1993

Fédération nationale des associations de consommateurs and the Public Interest Advocacy Centre, *Surveying Boundaries: Canadians and their Personal Information*,

Information and Privacy Commissioner/Ontario, *Privacy Alert: A Consumer's Guide to Privacy in the Marketplace*, 1994

Information and Privacy Commissioner/Ontario, *Privacy Protection Makes Good Business Sense*, 1994

Information and Privacy Commissioner/Ontario, *Privacy Protection Models for the Private Sector*, 1996

Information and Privacy Commissioner/Ontario, *Smart Cards*, 1993

Louis Harris & Associates, *The Equifax Canada Report on Consumers and Privacy in the Information Age*, 1992

Westin, Alan, *1996 Equifax/Harris Consumer Privacy Survey*, 1996