Contactless Smart Card Applications:

Design Tool

and

Privacy Impact Assessment

April 2007

Advanced Card Technology
Association of Canada

The Advanced Card Technology Association of Canada gratefully acknowledges the work of:

Catherine Johnston,
Neville Pattinson and Gemalto
and
Patrick Hearn and Oberthur Card Systems,

as well as the support of the ACT Canada Emerging Markets, Applications and Technologies Strategic Leadership Group.

We would also like to acknowledge and thank **Dr. Ann Cavoukian**, Information and Privacy Commissioner of Ontario (IPC) and her staff. This work would not be possible without the comments of the IPC and their assistance with the production of this publication.

ACT Canada and the IPC developed and co-published two earlier Privacy Impact Assessment Procedures. Working together, we have sought ways to promote advanced card applications and technology that are privacy enabling.

This publication is also available on the ACT Canada (**www.actcda.com**) and the IPC (**www.ipc.on.ca**) websites.

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

Table of Contents

Foreword

The Advanced Card Technology Association of Canada (ACT Canada) is a non-profit association that provides a voice for all advanced card applications, technologies and biometrics 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. These contact and contactless smart (also known as chip), optical also known as laser) and capacitive cards are in use around the world and are now used in Canada. The technology platform allows more information to be stored and transported than do the existing magnetic 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, USB tokens and others are emerging as personal information devices (PIDs). Applications using PIDs need to adhere to personal information protection standards.

ACT Canada is working with our members to develop this privacy design and assessment tool so that developers can build protection of privacy into applications using advanced card technology platforms and PID applications.[1] Because applications invariably require data to be collected, used, disclosed, retained, and destroyed, privacy must be designed throughout the entire system and this tool helps with each stage.

The Information and Privacy Commissioner of Ontario (IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act* (the *Acts*) to research and comment upon matters relating to the protection of privacy with respect to personal information held by government organizations. The Commissioner also plays a role in educating the public about privacy and access issues. 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.

With input and production assistance from the IPC, ACT Canada has developed this document to help companies and organizations understand and implement, in a practical way, the principles of privacy protection. We 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 needs.

This design tool and Privacy Impact Assessment (PIA) template provides readers with a basic understanding of fair information practices used in many countries to protect the informational privacy of individuals. It also provides a process whereby application owners, designers and others can incorporate privacy protection into your application design -- the easiest and most cost-effective time to deal with it. Throughout this document we use the term “you.” Generally this refers to the application owner, usually the organization that issues the card to the customer

1 This document will not address the potential of automated systems to provide ongoing systems management information and to ease reporting both on systems level privacy metrics, and to individuals who request information of the system.

or citizen. In some specific instances it will refer to the application designer. In a few instances it refers to you the reader, regardless of your role other than that of an individual who has expectations of privacy. 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

Executive Summary

Privacy protection is good business, providing a competitive edge for many organizations. It is also a legislated mandate in Canada and in a growing number of countries.

The most effective and economical time to incorporate it into your applications and systems is during the design stage. These strategic choices are related not only to the personal information that resides on your advanced card platform, but throughout your system, wherever it appears. Your corporate privacy policies, procedures and reporting complete the integrity of privacy protection.

This document will take you through each stage, outlining what you need to do, as well as your options. It not only helps you systematically design privacy in, but also results in documentation that can be used for marketing and certification purposes.

As the public and private sectors strive to offer new products and services, increase customer satisfaction and balance privacy and security, advanced card technologies provide the platform. This design tool will help you use their privacy enabling attributes.

Chapter 1: The Basics

What is Privacy?

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. It has several dimensions. One is protection of our personal data, also described as informational privacy or data protection. As individuals, we do not want data about ourselves to automatically be made available to other individuals or organizations. When another party holds our data, the individual must be able to exercise a substantial degree of control over that data and its use.

Privacy is often confused with the more commonly understood concept of confidentiality. Confidentiality refers to certain duties or obligations of individuals to safeguard information, with which they have been entrusted. In connection with computer systems it is also confused with security. In this case, security is used to protect data, but privacy protection goes beyond that and includes policies, procedures and compliance to regulations and legislation.

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, government 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 has sold it to another company, you might not know. In that case, you would find it very difficult to identify the new companies who now have your personal information, to check the completeness and correctness of that data, and to 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 to others about yourself. 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, not 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 customers' needs and expectations, is one of the central tenets of today's business environment.

Your customer is a source of valuable information whose privacy must be respected and whose data must be 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. In July 2006, the Privacy Commissioner of Canada released results of a survey conducted by Ekos Research. Key findings were that:

- Canadians are very concerned about the government's transfer of individual personal information across borders, by outsourcing work to companies in the U.S. and overseas.
- Only 50 per cent of those polled say they have enough information to know the privacy implications of new technologies.
- Canadians want to be informed by companies about the privacy implications of products or services they buy.

An earlier poll conducted in 1998 by Angus Reid concluded that Canadians overwhelmingly find it unacceptable for companies to sell, trade or share customer information with other companies. Similarly, Canadians believe 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 per cent want web policies that prohibit the sale of their data to other organizations. Ninety per cent want control over their personal data. More recently, a survey conducted by Yankelovich Partners, released in August 2000, found that 90 per cent of consumers felt the protection of their personal privacy is the most important issue associated with e-commerce transactions. Research by the Ponemon Institute in 2006 indicates that 12 per cent of people will change their online behaviour based on privacy issues on websites.

This concern for privacy is starting to affect business practices. When companies fail to respond to consumer concerns they can lose revenue and jeopardize customer relationships. Fortunately, companies are increasingly recognizing that responding to their clients' desire to control the use of their personal information makes good business sense that will provide a competitive advantage in the marketplace.

Privacy and Identity Theft

There is another compelling reason to protect our personal information. Identity theft is a serious consumer fraud. The U.S. Federal Trade Commission says it accounts for 40 per cent of all consumer fraud complaints. A September 2003 survey [2] for the U.S. Federal Trade Commission

2 See Synovate, *Federal Trade Commission - Identity Theft Survey Report* (covering May 2002 - May 2003), available at **http://www.ftc.gov/os/2003/09/synovatereport.pdf**

(FTC) found that within a one-year period nearly 10 million persons in the United States -- 4.6 per cent of the adult U.S. population -- discovered that they were victims of some form of identity theft. PhoneBusters, established in January of 1993, is Canada's national anti-fraud call centre jointly operated by the Ontario Provincial Police and the Royal Canadian Mounted Police. PhoneBusters is the central agency in Canada that collects information on telemarketing, advanced fee fraud letters (so called "Nigerian letters") and identity theft complaints. Their statistics show the extent to which complaints have been registered. What is uncertain is the extent to which this problem will grow as more and more personal information is stored electronically and becomes subject to attack.

Identity theft or fraud occurs when someone uses someone else's personal information without his or her knowledge to commit fraud or theft. It could be your information and the following could happen to you or someone else.

- They open a new credit card account, using your name, date of birth, and Social Insurance Number. When they use that credit card and don't pay the bills, the delinquent account is reported on your credit record.
- They call your credit card issuer and, pretending to be you, change the mailing address on your existing credit card account, then run up charges on your account. Because your bills are being sent to a different address you may not immediately realize there's a problem.
- They subscribe to a cell phone service in your name.
- They open bank accounts in your name and write bad checks.
- They can transfer bank balances, apply for loans, mortgages and other services, purchase vehicles, take luxury vacations, and do things you might think you can't afford.

Thieves can use your driver's licence, birth certificate, Social Insurance Number, and mother's maiden name along with other ID to convince people that they are you.

It is important to keep personal information out of the hands of criminals. There are several steps that consumers can take to minimize becoming a victim of identity theft, but the problem is largely out of their hands. Organizations have a growing need to protect personal information from external and internal threats. Those who collect massive amounts of personal information and leave it largely unencrypted, and in clear view of insiders and outsiders contribute to the problem. As stated in the IPC paper, *Identity Theft Revisited: Security is not Enough,* it is critically important that application owners (organizations) proactively protect the personal information of their customers and constituents.

Customers are becoming increasingly concerned about the loss and theft of data from corporate databases. By providing well thought out and implemented privacy protection, organizations may gain and retain more customers.

Identity Management and Form Factors

Today governments are placing more emphasis on identity management to protect citizens and to provide government-issued identification that citizens may use in their day-to-day lives. As technology evolves, it is likely that we will have more choices on how we carry our ID. Cards, as we carry today, are one form factor, but many other choices already exist. For example, the computer chip that resides on a chip (smart) card can also sit in a cell phone, PDA or USB memory stick. For that reason, although we talk about "cards" throughout this document, the principles and methods for protecting privacy apply to all form factors.

In order to manage identities, many governments, as well as companies, use the concept of an identity credential. This record of a person's identity, as determined by the body issuing the credential, may reside on any type of card or other form factor, as well as in a database or other electronic record. It may even be a paper based credential, although governments and corporations are moving toward more secure platforms to protect their citizens and customers.

There is another element of identity management. Consumers today are being spammed, phished, pharmed, hacked and otherwise defrauded out of their personal information in alarming numbers, in large part because there are few reliable ways for them to distinguish the "good guys" from the "bad" online. Application owners need to use all available means to help customers determine the legitimacy of all requests for personal information, as well as protecting that information in all instances, including when it resides on a card in the possession of the customer.

Contactless Technology vs. Radio Frequency Identification (RFID)

A contactless card is a smart card that uses radio frequencies to communicate with compatible terminals (readers) through the antenna embedded into the card. This differs from a contact card that is inserted into a reader so that data can be communicated. Contactless cards contain microprocessor chips that support various security tools, including encryption, to protect data as it is transmitted between the card and the reader. International standards allow contactless cards to operate at limited distances from less than a millimetre to 10 centimetres. For this reason, these are often referred to as proximity cards.

RFID tags are simple, low-cost and disposable electronic devices which are currently used to identify animals, track goods through a supply chain or to replace printed bar codes at retailers. RFID tags include an integrated circuit that typically stores a static number (an ID) and an antenna that enables the chip to transmit the stored number to a reader. When the tag comes within range of the appropriate RF reader, the tag is powered by the reader's RF field and transmits its ID to the reader. There is little to no security on the RFID tag or during communication with the reader, although the data on the chip may be encrypted. Typical RFID tags can be easily read from distances of several centimetres to several metres to allow easy tracking of goods. They are sometimes referred to as vicinity (read) cards or tags.

Switch Cards

New technology entering the marketplace incorporates an on/off switch built into the card. When a customer wishes to allow someone to read data from the card they press the switch. This allows the customer to control when data is available. The application owner should design their application to ensure that systems, while working with individual level data instead of in the supply chain or similar areas, are privacy-enabled end-to-end. This specifically means informing and engaging individuals so that they are making informed choices.

Contactless cards with an on/off switch allow consumers to control when their card information is accessed. Unless they press and hold the switch, which is built into the card itself, no one can access any applications or data on the card. This is true of all contactless switch cards, regardless of whether they use proximity or long-range read technology. It is important to note that not all contactless cards have switches. Also, the same privacy protection and security measures you choose for a non-switch card should be implemented on a switch card, for those times when the switch card is in an 'on' mode.

The Impact of Computer Technology on Privacy

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 viewed as 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 PCs 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. Decisions on sharing personal information cannot be made ad hoc, outside of privacy protection policies and procedures. Application owners must identify and take all steps to ensure that this does not happen.

Another security weakness is that data on one's PC is relatively easy to access. Just turning on someone's PC will often give you the ability to access his or her computer files, and today, hackers can break into networked computers from anywhere in the world. Again, adequate security must be employed to enforce the privacy policies.

It is important to recognize that security and privacy are not the same. Security is a risk management issue concerned with confidentiality of information, integrity of data and access

to data. The fact is that a security professional can assure confidentiality, integrity and access while still failing to protect privacy. Privacy is focused on the individual whose data is in the system, not the enterprise or the system and should account for:

- Consent – should be informed
- Purpose – should be defined and specific
- Use – should be only for defined purposes
- Disclosure – should only be by consent

These factors need to be built into data schemas and business rules right from the start.

Advanced cards allow individuals to carry more information in their wallets than they previously did. Smart cards are basically a PC on a credit card-sized 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, and like PCs, they are capable of running multiple applications. 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 music CDs and computer CD-ROMs. Canadians are currently using this technology for the Permanent Resident card.

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 payments, a person wants to know who will have access to their information about their purchases. With transit, a person wants to identify 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, transaction processing 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.

All this becomes more complex when contactless technology is used. The person carrying the card does not need to insert it into a reader, so may not always be aware of information being read. In most cases, the distance between the card and the reader is very small, so the consumer should be aware, but it is important for you, as the application developer or card issuer, to take additional steps to ensure privacy protection. It is important to note that in the case of identity management, most reputable technology providers make available technologies such as mutual authentication, as well as secure channel communication, to ensure that the transaction between the reader and the contactless card is secure.

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.

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 is "entered?" How do we ensure that the data isn't copied and given to others who were never intended to have access to it? As you address each of these, you must do so from the perspective of privacy, as well as security. After you have assessed your privacy requirements you will need to design security appropriate to enforce your privacy design.

Protection of privacy must be viewed systematically at each stage from collection to destruction. In each you must address the concepts of consent, purpose, use and disclosure. A critical element of enabling privacy is that data must be minimized whenever personal information is collected, used or disclosed. It also means that the person who is the subject of the data must be a central participant in determining what is done with the data. Security must be aligned with both the idea of data minimization and of data subject involvement in order to effectively facilitate privacy. For example, locking down access to data without role-based access or its equivalent may provide confidentiality, but is unlikely to aid privacy.

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 their information. In some cases they 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 concern for many people.

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 applications.[3]

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 (FIPs).

3 Should you wish to have a better understanding of advanced card technologies, you may contact the Advanced Card Technology Association of Canada, 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* or *FIPS*.

There have been several attempts to develop a complete and comprehensive set of FIPs. One of the earliest was undertaken in 1980 by the Organisation for Economic Co-operation and Development (OECD) in their *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Efforts in the 1990s to protect privacy included 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, and Québec's *The Act Respecting the Protection of Personal Information in the Private Sector*, which sets out fair information practices for businesses operating in Québec. The Canadian Standards Association's *Model Code for the Protection of Personal Information*[4] was created in the mid 1990s and is incorporated as the practices to be observed in Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA). Multinational organizations may consider looking at the Global Privacy Standards adopted by International Data Protection Commissioners Conference[5] or the Generally Accepted Privacy Principles (GAPP) that have been adopted by Canadian and U.S. accounting bodies.[6]

In *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.

4 A copy of the *Model Code for the Protection of Personal Information* (document code CAN/CSA-Q830-96) can be obtained by the Canadian Standards Association. A summary of the principles is included as Appendix A below.

5 More information on the Global Privacy Standard can be found on the IPC/O website at **http://www.ipc.on.ca/images/Resources/up-gps.pdf**.

6 See the Canadian Institute of Chartered Accountants website for a copy of the GAPP at **http://www.cica.ca/index.cfm/ci_id/33622/la_id/1/document/1/re_id/0**.

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

Accountability

Your organization must designate a person to be accountable for privacy, notwithstanding the requirement that each individual is also accountable for his or her own actions in the handling of personal information.

Communicate your privacy policies and practices to all staff, and train your staff to a level sufficient to enable them to reasonably and consistently recognize and respond to privacy issues and be 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.

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 there is 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 -- they should be transparent.

Develop and publicize a process for addressing and responding to any customer inquiry or complaint regarding the handling of his or her 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.** The purposes must be clear and understandable.

Do not withdraw access to services or products if your customers subsequently refuse to permit the use of their 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 it is reasonably possible.

Collect customers' personal information with the knowledge and consent of the customers, except in very limited circumstances, and inform the customers 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
- source(s) from which the personal information is to be collected, if not directly from the customer.

Notification must be clear and easy to understand. Short and/or layered notices should be considered to facilitate customer understanding.

Use

Only use personal information for the purposes identified to the customers at the time of collection unless the customers explicitly consent to a new use, or law authorizes the activity.

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 they are denied access, you should inform the customers of the reasons why and provide them with a fair opportunity to challenge the denial.

Where an incorrect inference has been made from the analysis of multiple sources of information, the customers 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 customers' personal information if it is found to be inaccurate, incomplete, irrelevant or inappropriate.

Make note in customers' files of any discrepancies regarding the accuracy or completeness of their 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 customer 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.

For more information on retention and disposal, please refer to the IPC Fact Sheet #10 on the *Secure Destruction of Personal Information*[7]. You might also refer to ***PHIPA*** order HO-001[8] regarding the inadvertent disclosure of health records in downtown Toronto as part of a movie shoot, due in part, to improper procedures.

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 so that an application controlling one set of information cannot access the information controlled by another application.

Aggregation

Where a company collects information about 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, behaviours, activities, or attributes of a customer without the prior permission of the customer.

Contractual Agreements

Stipulate clearly 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.

7 http://www.ipc.on.ca/images/Resources/up-fact 10 e.pdf
8 http://www.ipc.on.ca/images/Findings/up-ho_001.pdf

Anonymity and Pseudonymity[9]

Reduce, to the greatest possible extent, the collection and retention of identifiable transactions, i.e., those 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.

Pseudonymity - 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 where application data resides has equally adequate protection. This includes forms on which data is written or otherwise coded, databases and all other files.

9 It is important to assess the applicability of anonymized and pseudonymized transactions within a smart card deployment. Often the opportunity to allow for both the significant reduction in the collection and use of personal information is missed. Use of multiple IDs and PINS as well as biometrics and credential-based systems can be very privacy-protective and should be explored.

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. Privacy Impact Assessments (PIA) are typically assessments or reviews that are carried out as part of a systems requirements specification and design phases.

The following components make up a 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 that you as the application owner should take is bolded and italicized. 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 components. 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.

In preparing your response, you will not only specify the privacy protection you have designed, but you will also show how you incorporated it into your system, policies and procedures.

These requirements may require you to provide details of competitive intellectual property. Because of this, you may wish to keep your detailed PIA response confidential and reserved for audit purposes. An evaluation grid can be found in Appendix D. It should be used when your PIA is being audited and can be publicly used if you do not wish to make your detailed response widely available.

This is an example of a guiding checklist only, and should not be used as is without review against your specific requirements and regulatory environment. You should construct a detailed checklist for your own use, based on the technologies you will use throughout your system in all aspects to support your application. It should also take into account the specific personal information to be handled and account for any particular regulations that individual entities may be subject to, resulting in a checklist likely more granular and specific than that found in Appendix B.

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. It should be noted that the ACT Canada PIA for Contactless Smart Cards was the procedure used, so that the reader understands the criteria.

In the case of a multi-application card you may not initially know the final configuration of the multi-applications, as applications may be added post-issuance. The primary issuer is expected to take ownership of the multiplication nature of the card and should complete the PIA checklist for all the applications that are loaded pre-issuance. This may require working with the designers of the other applications.

Owners of the applications that may be loaded post-issuance should also complete the PIA checklist to ensure the overall privacy protection of all applications on the card. There may be some "firewall" issues here with respect to application independence and the lack of cross-application integration, but one way or another all parties should be making a conscious effort to ensure privacy protection of their application as part of the multi-application environment.

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. It is important to include 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. All applications must be included if this is a multi-application card, regardless of whether it uses a dual interface, contactless or hybrid card platform. This also applies to magnetic stripes, bar codes etc., as combination cards are generally the norm.

Security of Multiple Sources of Information

Describe the security mechanisms that prevent information leaking from one application to another, if there are multiple applications.

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, or some form of federated identity is used across more than one application or system, 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:

- information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
- 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;
- any identifying number, symbol or other particular assigned to the individual,
- the address, telephone number, fingerprints or blood type of the individual;
- the personal opinions or views of the individual except where they relate to another individual;
- the views or opinions of another individual about the individual; and
- 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 details as:

- does the information pertain to one individual or to a group of individuals;
- what is the approximate number of records to be collected for each customer; and
- 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 their 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 anonymizing or pseudonymizing techniques to minimize the need to collect or share personal information.

The purpose of collection needs to be identified for each and every application.

How is the 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, the individual should give informed consent, 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.

The nature of consent must be related to the sensitivity of the data. Sensitive data, such as personal health or financial information, must have explicit rather than implied consent[10], bearing in mind that consent is moot when access is required by law.

It is also key to ensure that the customers' 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. Notices must be clear, and in simple language to ensure that consent is informed.

You should be aware that it may be necessary to ask for a new consent from users when a new application is added to a card. This question should be viewed from the point of view of the consumer, not the developer.

10 Note that under *PHIPA*, consent for the collection, use or disclosure of personal health information can be implied for those health care practitioners providing health care to an invidual.

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 is a start and finish date 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 him or 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? Accuracy also refers to the timeliness and completion of data.

Method of Storage

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.

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, role, 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:

- the overall custodian of the data who is responsible for the ongoing assurance of privacy protection;
- the person responsible for answering questions or resolving customer complaints; and
- 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 and often at that point, it may be too late. Certain decisions may have been made during the development phase which means that access is either not possible, or prohibitively difficult or expensive.

Procedures for Complaints and Appeals to 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 their concerns to be addressed -- customer service at is best. These concerns may take the form of complaints about how their personal

information is being treated. The individual 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[11] 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.

You should also provide an audit trail of moves, additions, changes, deletions and accesses to personal information. This should, where feasible or practical, include who accessed the data and for what purposes.

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 a customer to select.

Describe the monitoring or process control system.

Describe the procedures or system by which you will monitor ongoing compliance to policy and access to personal information.

Retention and Disposal

Describe the rules or guidelines used to determine retention periods for personal information and the methods by which data will be destroyed.

Personal information should not be retained any longer than is required for reasonable business purposes, and as long as retention is required by law. As soon as requirements for retention have expired, data must be disposed of in a secure manner.

11 Timelines in this context need to be from the customer's point of view. For example, *PIPEDA*, Canada's *Personal Information Protection and Electronic Documents Act* uses the following: "An organization shall respond to a request with due diligence and in any case not later than thirty days after receipt of the request."

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, or modification, 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 is written on the card and is 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.

Card Audit Capabilities

Because smart cards have memory and processing capability and are capable of storing and enforcing rules of use and access, they are also capable of keeping an audit trail, if programmed to do so. This would be a useful privacy and security feature and should be considered as a part of your privacy program.

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 Only	Add Data	Change	Delete	Copy	Print	Communicate	Block Access
Card Owner Name	Card Owner	Y	N	N	N	N	N	N	N
	Issuer (Airline)	N	Y	Y	Y	Y	Y	Y	N
	Travel Agent	Y	N	N	N	N	N	N	N
Frequent Flyer Number	Card Owner	Y	N	N	N	N	N	N	N
	Issuer (Airline)	N	Y	Y	Y	Y	Y	Y	N
	Travel Agent	Y	N	N	N	N	N	N	N

Let's say the application is a health card[12]. Your fields might include the following:

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

It is important to identify each piece of data, but equally important to identify it by location. That is to say 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 backup. 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.

Monitoring or Process Control System

Describe the procedures or system by which you will monitor ongoing compliance to policy and access to ***personally identifiable information*** (PII).

Rules for Multiple Application Systems

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

Contactless Technology Considerations

Privacy protection requires bringing together technology, policies, procedures and the commitment of people to deliver the level of protection desired. If any one of these is missing, or weak, you have the potential for breaches. For example, you can design and enforce rules as to who accesses information contained in a citizen's travel ID. That includes reading data, adding, modifying and deleting it. When a citizen inserts a "contact" card into a reader, he or she is aware that a data transaction is taking place. When the card is contactless, the citizen may or may not be aware. This, in part, depends upon the range from which the reader can access the card's data. If it is a very short range (one millimetre to 10 centimetres), the citizen may be aware, because he or

12 Please note that in Ontario, any card that contains personal health information is likely to be required to comply with the *Personal Health Information Protection Act* (***PHIPA***). In the example given, the doctor role is not allowed to change drug allergies, but under ***PHIPA*** the doctor would be required to do so if the patient's condition changes. Similarly, in the example the patient is not allowed to block access, but under ***PHIPA*** a patient may specify who can and who cannot have access to parts of their personal health information. In other words, you are responsible for doing the due diligence to ensure that your application is compliant in the particular circumstances in which you and your customers find yourselves.

she may need to take their card out of the wallet and place it near the reader. When the range is greater, the risk increases that the citizen may not be aware of being "read."

To mitigate the risk of unknown 'reads', there are options. One uses a technology to block all access to the card data by placing the card in a form of shielded envelope. Until the envelope is "opened" the data is not accessible. The designer must determine whether it is acceptable to make the cardholder responsible for privacy protection through the use of the shield, taking into consideration whether the shield would preclude carrying the card in a standard wallet. Where there is a risk that the cardholder would not employ the shield, other options should be considered. The user should always be aware that his or her information is being accessed or attempted to be accessed, by virtue he or she must perform an action to start the process, for example, enter a PIN; insert the card; hold it next to a reader; swipe the card in some way to read something from the surface of the card to wake up the Radio Frequency (RF) part of the chip, etc.

In the case of RF based communication protocols, the card should always issue a random number on activation in the reader field, ensuring that no association is possible to the card or individual, and then a mutual authentication is performed between the reader and the card ,followed by encrypted RF data transmission of only the data authorized to be read by the external application.

It is critical that policy, procedures, audits and enforcement are in place to ensure that all persons authorized to access data for specific purposes, such as a border crossing, are prohibited from using that authorization at any other place or time. Ensuring that there is no unauthorized use of the reader device, no excessive usage of the device and no disclosure of confidential information, is critical.

In this case, it would be helpful to automatically store an audit log on the card of every person who has accessed data, recording what was done and when.

Contactless technology can also utilize Basic Access Control (BAC) to ensure the individual has control over the activation process of the chip. It is also possible to utilize biometrics as an access control, before transmission of information between the card and reader (a more sophisticated example of BAC). Finally, one can also put in protocols that temporarily deactivate the contactless capability of the card.

Designers may also use dual interface technology to limit the type of information put in the contactless side of the chip. The firewall between the contact and the contactless side ensures unauthorized access to other information of the chip is kept out of bounds from would-be hackers, etc.

Chapter 5: The Process of Implementing and Maintaining a Privacy-Protective System

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, typically your Chief Privacy Officer (CPO). Alternatively, 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. 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 CPO 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. Educating 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

You've planned, built and implemented a privacy-protective system and now there are a number of steps to take to maintain or monitor its effectiveness. Establishing baseline metrics, along with targets for compliance and alarm thresholds, and typing metrics to managerial performance measurements will go a long way to ensuring consistent and transparent enabling of privacy.

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 would give you an opportunity to acknowledge good practices and correct poor ones. A periodic review of your corporate policies and procedures will reinforce your 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.

Lastly, you need to remember that any changes, such as adding new applications to a card, changing any of your privacy protection principles or how they are implemented, or changes to your policies and procedures will require a review and possible involvement of the data subjects. For example, if you decide to use information in a way that was not on the original consent form, you will need to obtain new consent. A change in key privacy personnel may result in updates to your privacy statements on your web site and elsewhere.

Evaluation Phase

Independent evaluation or audits of the privacy functionality of a smart card system, using generally accepted standards appropriate to your application, is necessary. Without independent evaluation the vulnerabilities of the system will be embedded, but unexamined.

Conclusion

We hope that throughout this process you have thought about your own personal information and how important it is that no company misuses 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.

As an example of what can go wrong when caller identification applications were first introduced, many companies assumed that responding to customers by name when they called would be seen as good customer service. They soon found that people often did not take kindly to that approach. “How do you know my name?” expressed in angry tones, was frequently heard.

We all value our privacy in a general sense and we are becoming more sensitive about the protection of our information. ACT Canada has, through this paper, provided the tools to make privacy work for you.

Appendix A: CSA Model Code

Canadian Standards Association

Excerpt from the Model Code for the Protection of Personal Information[13]

4. Principles

4.1 Principle 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.

4.2 Principle 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.

4.3 Principle 3 — Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. **Note:** *In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.*

4.4 Principle 4 — Limiting Collection

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

4.5 Principle 5 — Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

13 The complete code can be found at **http://www.csa.ca/standards/privacy/code/**. Note that the OECD guidelines are an appendix to the CSA code on this site.

4.6 Principle 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.

4.7 Principle 7 — Safeguards

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

4.8 Principle 8 — Openness

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

4.9 Principle 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. **Note:** *In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.*

4.10 Principle 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.

Appendix B: Example Privacy Protection Assessment Checklist

	STEP	Completed
1.	**List Applications** List all applications, including all common data fields that are separate from the applications e.g.: Driver's Licence Health Information Social Benefits Common data: name, address, birth date	
2.	**List Data or Conclusions that can be Inferred** e.g.: cardholder receives social benefits because the application resides on the card, or birth date can be derived from access to the driver's licence number	
3.	**Description of the Proposed Application(s)** *Describe the proposed application(s) requiring the collection of personal information.* ▪ What are the important features? For example, what categories or groups of individuals will you gather information from for your application and what classes or types of information will be 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?	
4.	**Description of the System** *Describe how the application(s) reside within the overall system.* Flow charts may be used, if appropriate, to show how data flows between people, devices and functions.	

	STEP	Completed
5.	**Description of the Personal Information to be Collected** *List and describe the personal information to be gathered. This should be organized by the records in which the data is stored. Some data fields may appear in multiple records.* What type of personal information is to be collected? ▪ How is the information obtained (directly from the source or indirectly – for example, from a doctor or employer) and is any third party information involved, for example, an agency that has been contracted to conduct reference checks? 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? For example, does your application require different information based on the person's gender or age? 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? For example, a driver's licence will have one data record that pertains to the driver's right to operate a motor vehicle, but may also have multiple records related to demerit points.	
6.	**Purpose of the Collection** *Identify the purposes for the collection of personal information.* ▪ 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, 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? For example, are you collecting a customer's address to deliver a product (functional) or update a database record (administrative).	

	STEP	Completed
7.	**How is Notice of Collection Given and Informed Consent Obtained?** *Design the notice to be authorized by the customer, and attach. If consent is sought and given electronically, provide the messages and show the process to be followed.* ▪ 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? If yes, please provide details.	
8.	**Method of Collection** *Describe how information will be collected and, if appropriate, how it will be linked to previously collected information.* You may collect initial information at the start of the program and then add more throughout the life of that program. Both should be addressed here. ▪ What is the process of collection? For example, is it entered by keyboard, read from the smart card or transmitted from another computing device? ▪ How is the collected information transferred (if appropriate) 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?	
9.	**Duration of the Collection of Personal Information** *Identify the period of time over which the data will be collected.* ▪ Is the collection for this one time only, is it limited in duration, or ongoing? ▪ It is particularly important to note the reasons why any collection is ongoing, as this leads into issues of data integrity.	

	STEP	Completed
10.	**Accuracy** *Outline the steps to be taken to ensure that information is accurate at all stages of the application.* ▪ 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? Note that accuracy also deals with timeliness and completeness. Steps are required to enable a person to rectify out-of-date or incomplete information. ▪ Is a verification process part of the overall process?	
11.	**Method of Storage** *List each method by which the personal information is stored, including the original collection form, computer files and copies, backup copies, printed reports, on the advanced card, etc.* Storage includes temporary and long term; for example, information may be stored on a device until such time as it is moved to another device.	
12.	**Key Personnel** *List by name, role and title all personnel responsible for the privacy of this application and in your organization.* ▪ Who is the Chief Information Officer of the organization i.e., the person who serves as the focal point for the privacy protection process? If that title does not exist, who is the person responsible for privacy within your organization? ▪ Who are the people who have roles in the access and correction process? ▪ From the perspective of those inside the organization, is it useful to list persons who have key roles in the functions of collection, use, retention and disclosure of the information? Also, who are the people explicitly responsible for privacy in development, Quality Assurance and operations?	

	STEP	Completed
13.	**Description of Procedures for Access and Correction.** *Describe the process to be used by individuals to view and request changes to their data.* ▪ What procedures will be used 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 that outlines the steps of the access process and correction process for staff. ▪ Is there an appeals procedure? If so, outline the procedure.	
14.	**Procedures for Complaints and Appeals to 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.* ▪ What procedures are in place for customers to voice a complaint about how their personal information is being collected and used? ▪ What procedures exist if access to their information, or correction of it, has been denied? How are concerns resolved? What time frames exist for resolving them?	
15.	**Security** *Describe the security measures that will apply to the information at all stages of its existence. (See "Method Of Storage.")* ▪ 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. ▪ All contactless technology methods used to ensure privacy protection within the application(s) should be described here.	

	STEP	Completed
16.	**Retention and Disposal** ***Describe the rules that apply to determine how long each type of information shall be retained by the organization.*** ▪ What are the business reasons for retaining data? ▪ What regulatory requirements are there for data retention? ▪ Are there other reasons for retaining data, such as professional requirements (e.g. clinical reviews by practitioners)? ***Describe how the various types of data (electronic and physical) will be destroyed by the organization once the retention period has been reached.*** ▪ Are there regulatory requirements for shredding size? ▪ Are there regulatory requirements for types of disk wiping? ▪ Is physical destruction of electronic media required? ▪ Give precise minimum specifications for both physical and logical destruction of data (e.g. 3mm cross-cut shredding, 3 pass hard drive wipe with forced writing of 0 blocks).	

Appendix C: Example Data Field Checklist

Each data record should be represented in this checklist or in your data dictionary. The same data field may exist in more than one record.

Data Record									
Data Field	Accessed By	Read Only	Add Data	Change Data	Delete Data	Copy	Print	Comm-unicate	Block Access

Appendix D: Evaluation Grid

Contactless Smart Card Privacy Impact Assessment

ACTA FAIR INFORMATION PRACTICES	Pass	Exceeds Requirements	Fail
1. Accountability			
2. Recognition and Respect for Privacy			
3. Openness			
4. Purpose Specification			
5. Collection Limitations			
6. Notification			
7. Use			
8. Right of Access			
9. Right of Correction			
10. Accuracy			
11. Disclosure			
12. Retention and Disposal			
13. Security			
14. Aggregation			
15. Contractual Agreements			
16. Anonymity and Pseudonymity			

PIA SUBMISSION	Pass	Exceeds Requirements	Fail
Application Listing			
Description of the Proposed Application			
Description of the Personal Information to be Collected			
Description of the System			
Purpose of the Collection			
Notice of Collection and Informed Consent			
Method of Collection			
Duration of collection			
Accuracy			
Method of Storage			
Key Personnel			
Access and Correction Procedures			
Complaints and Appeals Procedure for Denial of Access or Correction			
Security			

Glossary

Advanced Card - A card capable of carrying information. Uses technology more advanced than magnetic stripe. (See magnetic stripe, optical card, capacitive card.)

Anonymity - Anonymity in this context refers to the complete absence of identification 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 capacitively coupled memory card.

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, to individual or corporate cardholders.

Cardholder – This is generally the person to whom an identification card is issued. For financial transaction 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.

Contactless Card: Smart card that uses radio frequencies to communicate with a compatible terminal through the antenna embedded into the card.

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, PDAs, 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 a laser card, because a low-intensity laser is used to burn holes of several microns in diameter into a reflective material exposing a substratum of lower reflectivity. The presence, or absence, of a burned hole represents bits. The areas of high and low reflectivity are read using a precision light source.

RFID tag: Simple, low cost and disposable electronic devices that are used to identify animals, track goods logistically and replace printed bar codes at retailers. RFID tags include an integrated circuit that typically stores a static number (an ID) and an antenna that enables the chip to transmit the stored number to a reader. When the tag comes within range of the appropriate RF reader, the tag is powered by the reader's RF field and transmits its ID to the reader. There is little to no security on the RFID tag during communication with the reader. Typical RFID tags can be easily read from distances of several inches to several yards to allow easy tracking of goods.

Smart Card - A credit card-sized piece of plastic with an embedded computer chip. i.e., capable of calculation.

Bibliography

ACT Canada & Information and Privacy Commissioner/Ontario; *Smart, Optical and Other Advanced Cards: How To Do A Privacy Assessment,* 1997 (available on www.actcda.com)

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

Cavoukian, Ann and Hamilton, Tyler J; *The Privacy Payoff, 2002*

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

Johnston, Catherine, (the following are available at www.actcda.com)

> *Where Do We Go Now? (10/01/01)* The issue of privacy vs. security in the aftermath of the September 11 terrorist attacks.
>
> *Privacy and Security* 06/08/01 The issue of privacy and security surrounding electronic fraud in Canada: statistical analysis and privacy protection utilizing advanced card technologies, including security tools such as biometrics and encryption
>
> *E-terrorism, Privacy and Trade: What do they have in Common* 2002
>
> *Privacy and Smart Cards*, 2001

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

Advanced Card Technololgy Association of Canada
85 Mullen Drive
Ajax, Ontario L1T 2B3
905-426-6360
Fax: 905-619-3275
Website: www.actcda.com
Email: info@actcda.com

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
Email: info@ipc.on.ca