The Security–Privacy Paradox: Issues, Misconceptions, and Strategies

A Joint Report by

The Information and Privacy Commissioner/Ontario

and

Deloitte & Touche

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

Deloitte & Touche
Deloitte & Touche

August 2003

Ann Cavoukian, the Information and Privacy Commissioner of Ontario, gratefully acknowledges the work of Mike Gurski in preparing this report.

This publication is also available on the IPC website.

Information and Privacy Commissioner/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

Deloitte & Touche
181 Bay Street
Bay Wellington Tower – BCE Place, Suite 1400
Toronto, Ontario, Canada M5J 2V1
416-601-6150
Fax: 416-601-6151
Website: www.deloitte.ca

Table of Contents

Introduction

Organizations that use the personal information of individuals are increasingly confronted by the question of privacy, either through legislation, industry self-regulation, or customer expectations. Many commit to addressing the question. Yet they still face one particularly confusing and troublesome issue: the complex and largely undefined relationship between the disciplines of information security and privacy protection.

These disciplines overlap and contradict, and, therefore, can be paradoxical. In preserving one, companies may do serious damage to the other. Complying with one set of regulations may mean unintentionally violating others.

This paper seeks to clarify the security–privacy paradox for senior executives and other professionals by:

- Describing and illustrating major characteristics, points of difference, and areas of overlap between information security and privacy protection.
- Addressing issues and misconceptions that can lead to wasted money, time, effort, conflict and, all too often, inappropriate measures and programs.
- Suggesting and prioritizing business, organizational, and technical approaches that are cost-justifiable and can be beneficial in reaching regulatory compliance.

This paper deliberately puts greater emphasis on the privacy side of the equation, because privacy protection involves concepts and principles that executives today may find less familiar or less well defined. This is not a judgment of the relative importance of security or privacy. In fact, in many enterprises and global networks, concerns for information and process security affecting non-personal data will likely dominate corporate agendas for years to come.

However, the evolution of the computer from background record-keeper to interactive, networked transaction manager has increased dramatically the volume and variety of personally identifiable information collected and held by organizations. This capability for high speed, high volume processing and dissemination creates the potential for substantial risks, as well as large-scale opportunities, associated with information security and privacy protection.

Security and Privacy—Peeling Back the Layers

For the purposes of this paper, *information security* refers to the controls deployed by the organizations or their surrogates for the purposes of securely collecting and holding data. It applies to personal and non-personal data alike.

Privacy protection, conversely, applies only to personally identifiable information and how the rights of an identifiable *data subject*—the person providing the information—are affected and enforced. Depending upon the industry, this may describe either a major portion of the data held by an organization, or only a small segment.

In the United States, the prevailing concept in the private sector is that once an individual provides personal information to an organization, the organization is the *data owner*, as well as the *data user*. U.S. firms often consider that the data they collect becomes their property and that they have the right, barring any sector-specific privacy legislation, to determine the use of it.

In European and Canadian-based privacy regimes, the individual is usually referred to as the data subject. The data owner designation in this privacy regime does not automatically cede to the organization that collects and processes or manages the data. Instead, the data subject retains certain rights, and the data user has the responsibilities of a custodian for protecting that personal information.

Regardless of what regime an organization adheres to—and multi-nationals may need to adhere to more than one—the challenge of maintaining a trust relationship with consumers remains the same. Adequately addressing privacy issues plays a key role in maintaining or developing that trust relationship.

Overlaps Between Security and Privacy

The commonly accepted elements of information security today are:

- Confidentiality—keeping information from others
- Integrity—ensuring that the information has not been changed without permission
- Accuracy and availability—the information can be accessed at the organization's request

A more detailed list of elements often used to define security functions adopts the functions of cryptography:

- Authentication
- Authorization
- Confidentiality
- Data integrity
- Non-repudiation[1]

The internationally accepted standard for defining information privacy can be found in the Fair Information Practices (FIPs) set out by the Organisation for Economic Co-operation and Development (OECD).[2] Eight elements comprise the FIPs:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

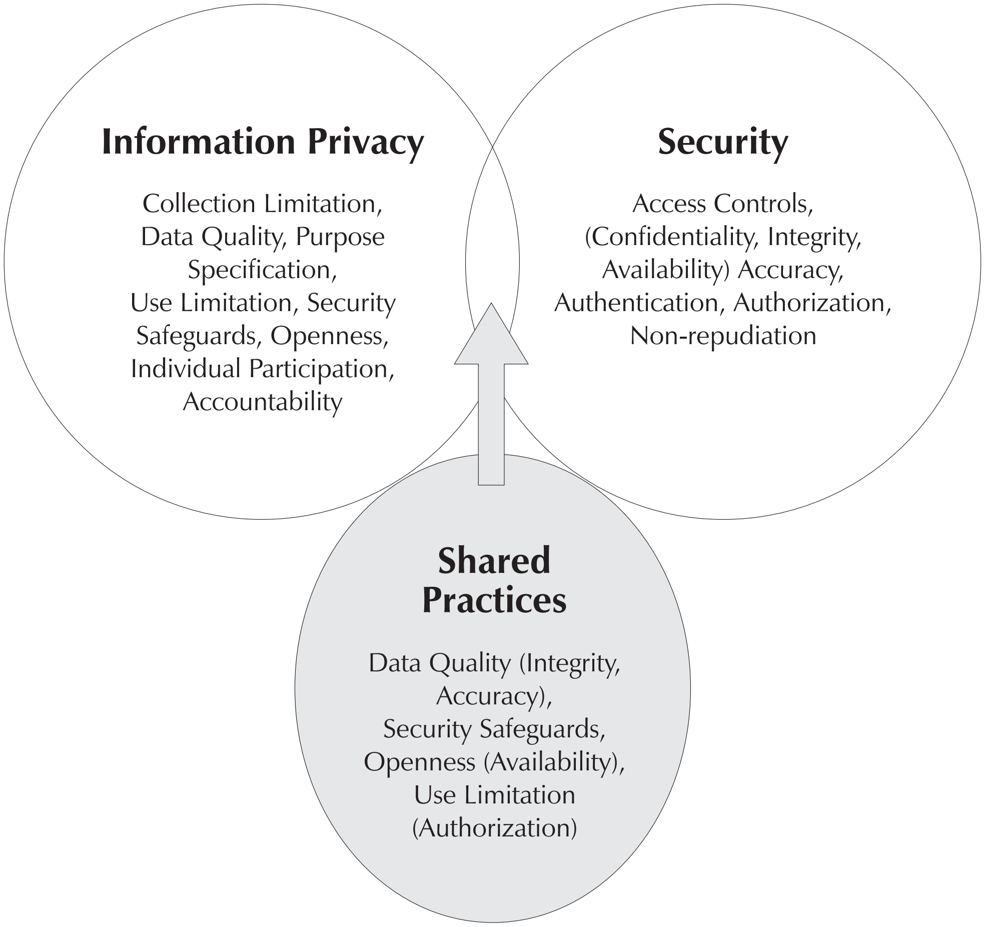
In some instances, such as the Canadian Standards Association's *Model Code for the Protection of Personal Information*, these elements have been expanded upon. Others, notably the U.S. Federal Trade Commission (FTC), focus on a simplified version of the OECD FIPs.[3] In this context, information privacy can be thought of as a set of controls placed upon organizations over the uses of personal information in their custody and control, and the rights conferred upon individuals over their personal information. What becomes clear in mapping out these security and privacy elements (see Figure 1) is that some of the components of privacy protection can be addressed by security safeguards, while others cannot. Some security functions may actually hinder or even threaten necessary privacy protection. Some privacy measures may weaken or threaten justified security measures. Hence the *security–privacy paradox*.

[1] Garfinkel, Simson, Web Security, Privacy and Commerce, O'Reilly, Cambridge, 2002, p. 80.

[2] www.oecd.org.

[3] For a concise explanation of the elements that define informational privacy see: Cavoukian & Hamilton, *The Privacy Payoff*, McGraw Hill Ryerson Inc. Toronto, 2002. pp: 44–53. For an introduction to the questions an organization needs to ask itself in managing privacy effectively go to: http://www.ipc.on.ca/PDT/. This tool is built on the CSA Model Code.

Figure 1: Results of Mapping the Elements of Information Security and Privacy


Information Privacy
Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability
Security
Access Controls, (Confidentiality, Integrity, Availability) Accuracy, Authentication, Authorization, Non-repudiation
Shared Practices
Data Quality (Integrity, Accuracy), Security Safeguards, Openness (Availability), Use Limitation (Authorization)

The Economics of Privacy

Regardless of the specific standard involved, today's privacy protection principles strongly assert that individuals should be able to exercise control over the accuracy, completeness, timeliness, use, distribution, and disposition of their own personal information.[4] While many agree that this assertion makes sense, it has neither guided many corporate privacy strategies nor been readily accepted in all social or political venues. Why not?

The direct and indirect costs of dealing with information privacy can be significant, whether it be for compliance with regulations or in response to a situation in which the organization is perceived to have breached an individual's or a group of individuals' privacy. No wonder that in the minds of many corporate executives, privacy is a lose-lose issue, viewed solely as risk aversion.

[4] There is a need for research, common sense, co-operation with appointed authorities, relationships within your own industry and intelligence as to how the public is moving on this subject.

Either way, an organization sinks significant operating funds and resources into global compliance programs to satisfy conflicting regulations. Erroneously, privacy management is often seen as a bothersome and expensive bit of overhead. Yet there is a positive aspect that many companies miss. It deals with brand image and trust.

Some forward-looking enterprises are using their privacy programs as public demonstrations of their concern for fair dealing. They go well beyond the compulsory compliance statements to show how and why they take care of their customers' personal information. For these companies, trust is a major market differentiator.

Privacy protection, properly executed and displayed, plays a major role in building trust. The simple reason is that customers' privacy expectations need to be met. Otherwise, their trust will be lost.

Organizations like the Royal Bank of Canada, also known as RBC Financial Group, have found that a portion of their business and profits are directly tied to how they manage privacy. Their research indicates that customers rate explicit privacy measures as a solid "second tier driver." In fact, privacy drives an average 6.9% of customer demand, making it a significant contributor to shareholder value.[5]

Privacy protection, as a cost component and competitive differentiator, needs more serious consideration in the marketplace.

Employee Privacy

Another aspect of privacy that is growing in importance is workplace intrusion. Stories abound today about corporate retention of e-mails, phone and workstation monitoring, surveillance cameras, and even the use of GPS devices for keeping track of individuals. Coupled with the traditional (and not so traditional) access management techniques used in many enterprises, these security and management efficiency techniques can create an atmosphere of Big Brother-like control.

Employee privacy rights and the enterprise's security and operational requirements can, and often do, conflict. In fact, this conflict represents one of the most classic cases of security–privacy paradox.

The solutions are highly situational, depending on the enterprise's security needs—e.g., defence, medical care, financial services, or gaming—and the contractual and legal rights of the employee. At the same time, these privacy and security issues cross borders, cultures, and economic interests. They are especially sensitive given the current focus on terrorism, both cyber and physical, as well as company failures.

[5] Peter Cullen, Chief Privacy Officer, RBC Financial Group, *A Matter of Trust*, May 27, 2002.

Security and Privacy Must Be Addressed

Clearly, the conflicts and dissimilarities between data security and privacy protection can be significant and difficult to harmonize. In a period of economic belt-tightening, it is tempting to push these confusing issues into a corner and only deal with them tactically and on demand, such as in response to attacks, direct requirements for regulatory compliance, or threatened lawsuits.

But in today's digital world, where more and more companies are sharing data in order to gain competitive advantage in their markets, the management of the security–privacy paradox takes on increasing importance. As a result, it should engage everyone involved in the information creation, exchange, processing, and storage that propels the enterprise.

Issues and Misconceptions

Operating on the premise that security and privacy are business matters that need to be managed, perhaps one of the most important services this paper can provide is to address some of the common issues and misconceptions surrounding them. In this way, the importance of information security is reinforced, while at the same time, the value of privacy as a business driver can be recognized.

Are Privacy and Security One and the Same?

Consider an organization in which privacy and security are considered to be essentially the same, without any distinction as to programs, policies, administrative structure, regulatory compliance, and technological design and implementation. These organizations often share characteristics. They have well established security processes. Many began existence with little direct contact with the public or individuals. They often deal in "things," not people.

Security is often viewed by such organizations primarily as a technical issue. Access management is often regarded as the major, if not only, security process. Since both privacy and security involve controlling information access and usage, this trap is easy to fall into. But it ignores the possibility that rigorous security processes may actually contribute to a mistaken privacy policy by making it impossible for data subjects to have the access to which they are entitled under privacy regulations. The problem with continuing to follow this approach is that privacy is never addressed. This creates vulnerabilities that could be costly, ranging from legal battles to lost customer trust.[6]

Actually, privacy protection includes a different set of protections than does security, as illustrated by Figure 1. By taking the approach of differentiating privacy from security, privacy protective functions will receive the appropriate analysis and resources necessary to design and deploy privacy protective information technology, and thus maintain and build customer trust.

A good example: In the Dutch Hospital Information System (HIS), a patient's private information is protected through the use of encrypted identification numbers, which create pseudonyms in place of actual identities.[7] Once a user successfully logs-in as a PC (personal computer) client, the correct patient is identified and his/her unique identifying number is passed from the server to the client. This number is encrypted to a value that is the pseudo-identity of this patient. Using this pseudo-identity, the required table containing the medical record can be accessed while maintaining the patient's privacy.

[6] The media abounds with examples where privacy interests were never considered and organizations get slammed for their lack of due diligence.

[7] "Guaranteeing requirements of data-protection legislation in a hospital information system with PET," Gilles van Blarkom, *The British Journal of Healthcare Computing and Information Management*, 1998 15 (4).

Not only does this system comply with all the requirements for mandatory data protection called for by the European Union's Directive on Data Protection, but the encryption process is performed at no measurable cost and has no adverse effect on the performance of the application.

This example demonstrates that enterprise privacy solutions have already been implemented with no discernable costs when designed into the system from the beginning. This is no longer new ground.

True or False: Privacy is a Policy Issue—Security is a Technology Issue

The policy-technology dichotomy is prevalent among renowned privacy experts—not just the security experts that propound this notion. The head of a leading Public Key Infrastructure vendor recently included in his presentation a slide that explicitly stated the viewpoint, and thus he completely eliminated any role for privacy-enhancing technologies or privacy architecture.

A subtler example is in the development of Privacy Impact Assessments (PIAs). These are tools that ideally look at both the policy and technology risks in a program or system with respect to privacy. In practice, PIAs tend to be policy-focussed—they rarely address information management and technology design issues. So, obviously, privacy experts also appear to fall prey to this misconception.

The problem with acting on this misconception—and it is a misconception—is that an organization can end up with technology solutions that allow the misuse of personal information by authorized personnel and authorized third parties. In addition, an organization can be lulled into a false sense of security, because it might have strong privacy policies but not have them backed up by deployed technology.

For example, an organization may post a privacy policy on its Web site, but does it ensure that the data collection controls for its Web forms are in compliance? Alternatively, it may have in place privacy invasive technologies that collect customer information, unbeknownst to the customer.[8]

Privacy is more than a technology issue. There is a growing body of privacy protective, enabling, and enhancing technologies[9] that are market-ready, especially in Europe and Canada.[10] For example, privacy-enhancing technologies (PETs) are tools that enable users

[8] RealAudio was a case in point when it was found to have highly privacy intrusive technology at play and in complete contradiction to their stated privacy policy. http://abcnews.go.com/sections/tech/cnet/cnet_realsuit991110.html.

[9] *Report on the OECD Forum Session on Privacy-Enhancing Technologies (PETs)*, December 3, 2001, Committee for Information, Computer and Communications Policy, Organisation for Economic Co-operation and Development.

[10] In Canada, firms such as Prescient have privacy protective database solutions that encrypt the relationships between data tables within a database. Zero-Knowledge has developed privacy rights management tools.

to make informed choices about privacy by providing them with control over their personal information. PETs can also satisfy legislative obligations and industry standards. Indeed, as PETs become more prevalent, they will increasingly influence the implementation of international privacy standards.

Designing privacy into a product or service will dramatically improve individuals' ability to control their personal information, in turn, increasing a product or service's commercial appeal. The truth is that IT systems currently have the resilience to handle privacy safeguards. Regardless of whether designers elect to implement PETs now or wait until legislation requires such technologies, PETs will become more of a reality for IT systems.

The implication of this is that an organization's privacy policy can be enforced through its deployed technology. This will provide a solid base from which to distinguish the competitive value of the organization.[11]

Privacy—Is It Really "Someone Else's Problem"?

Pushing the responsibility for privacy upstream or downstream is an especially prevalent attitude in network environments. There, service providers, enterprises, and other third parties combine to provide a complex set of business processes to other business entities and to the consumer.

Consider a relatively "simple" transaction like the purchase of a new car. Assuming the vehicle is either financed or leased, there are a series of transactions surrounding the sales event, all of which have some privacy content. Who are the business and institutional entities involved in the sale? The dealership, a finance company that may or may not be represented by the dealer, a credit rating system, an insurance company, a licensing agency, a tax entity, the dealer's affiliated service department, and the manufacturer and its distribution network. What information is involved? The buyer's personal identity—social insurance number or equivalent in the United States—home address, financial rating, type of intended use, yearly mileage, driver's license, driving record, ID of any underage drivers, and the vehicle's ID and vital statistics.

Who is responsible for protecting this information? The obvious answer is "all of the above." Yet the realistic answer is: "Who knows?" Consequently, the first question for any privacy-related, and most security-related, transactions should be: "Who is involved?" The second and more cogent question is: "Together and separately, are they providing seamless and appropriate protection?" The weakest link analogy applies very strongly here.

[11] Following use of one of its products, Real Audio was found to be surreptitiously collecting personal information. In response, Microsoft was quick to launch a PR campaign pointing out that Windows Media Player did not collect and send personal information to Microsoft with each use.

The problem with an enterprise operating on this misconception is that the other company may not be taking care of privacy protection. Privacy protection can thus fall through the cracks or be inconsistent, non-existent, or conflicting. Finger pointing, in the event of a privacy breach, is inevitable, and liability induced by association is highly likely.

Like it or not, one or more entities—usually the one with the deepest pockets and most likely to take a litigation hit—must view the network and process as a connected whole and analyze the regulatory, marketplace, public image, brand, and customer relations implications. This organization must then negotiate a solution—contractual, procedural, and technological—to deal with it.

A realistic approach will produce appropriate damage control and, more importantly, a much higher level of customer or partner satisfaction. This can then contribute to a positive brand image and recognition.

Which is Worse: The Wrong CPO or No CPO?

In organizations without a CPO, legislative privacy requirements, privacy compliance, and providing a contact point for complaints from the public can present strategic and chronic vulnerabilities for an organization. In other organizations, it is not uncommon for a Chief Security Officer or Chief Information Officer to take on a second hat—that of Chief Privacy Officer—once privacy protection becomes an issue.

The problem with merging the CSO and CPO responsibilities is one of differing views. The CSO tries to optimize organizational control, often starting from a security perimeter mentality. The CPO tries to ensure that the individual maintains control and that authorized users do not misuse data. Both perspectives need to be heard equally. When the position is combined, a security expert usually fills it. As a result, the privacy perspective is too often diminished or encoded into security items, before the issues are presented to the CEO.

The reality is, most organizations today that collect or manage personal information need a CPO. The CPO needs a working knowledge of data collection, data processing, and information management. The CPO really needs to know the business strategy and key success drivers of the organization, as well as public expectations and legislative context. This is a fundamentally different skill set than that traditionally held by CSOs. Security and privacy perspectives need to be independent of each other and be given equal voice to senior management. Only then can sound business decisions be made.

Having a CPO, independent of security or IT responsibilities, gives an organization an indispensable tool to deal with increased enforcement by regulatory bodies such as Privacy Commissioners, Data Protection Authorities, and the Federal Trade Commission. It will also assist organizations in dealing with privacy-related lawsuits and the increasing requirements of various pieces of privacy legislation. These often call for designated officials to be responsible for the implementation of privacy policies.[12]

The CPO position also creates the ability to properly address customer privacy issues and more importantly, embed privacy protection within the culture of the organization. This results in greater business strength, because the CPO becomes a catalyst for helping build that critical relationship of trust.

Privacy—Far More Than a Public Relations Exercise

Recently a company, after publishing its Web privacy policies, revealed that its privacy practices could differ from its stated Web policies. This soon became a public relations challenge and the company had to issue a statement to the effect that it would stand behind the stated privacy policies.

Many other examples have come to light in recent years in which organizations publicly state one position with regard to information privacy, but in fact, act differently. Organizations get drawn into believing their own marketing and public relations missives. They believe that the worst-case scenario ends with a senior executive who publicly announces that their customers' privacy is important after the company has been exposed for some egregious privacy breach.

Yet to get a sense of how many organizations fall into this trap, simply type "privacy glitch" into any Internet search engine. The results are quite striking. A number of companies have suffered significant embarrassment, loss of marketshare, and—in the worst instances—the pain of class action lawsuits and other governmental actions against them for breaching their own privacy policies.

This mentality must be replaced with privacy action items and privacy priorities. Changing to an action-oriented program will ensure that the organization is successful in addressing privacy issues. It also means the organization will benefit from being a privacy leader.

[12] For an examination of the CPO, the rationale for having one and what the roles and responsibilities of a CPO should be, see: *The Privacy Payoff*, by Dr. Ann Cavoukian and Tyler Hamilton, McGraw-Hill Toronto, 2002. pp. 125–151.

The Downside of Following the Leader

Organizations often justify the level of expenditure on security by benchmarking industry practices and using this benchmark as a strategic direction. While this approach may give some meaningful guidance for security, it is not a very reliable way to deal with privacy in today's environment. The problem is that individual competitors and whole industries may not be any more enlightened or mature about privacy than the average company. Plus, one size does not fit all with privacy. There are too many variables, ranging from the enterprise's global deployment, image sensitivity, prior record, risk aversion, and marketplace strategies, to use averages as a strategic director.

Benchmarking can—and perhaps should—be conducted. But those benchmarks should be used as a form of reality testing, a good source of competitive analysis, and possibly a source of market differentiation. Privacy standards are part of an organization's overall corporate image that is being promoted to customers, either explicitly or implicitly, by statements and actions. Either way, it's that image which is on the line.

Do Individuals Really Care About Privacy?

Offer customers a $5 discount on their fast food in return for some consumer information and business will likely be brisk. But offer that same $5 discount in exchange for the names of customers' children and the addresses of their daycare centers, and privacy will become a huge issue.

Privacy is, in reality, a volatile value that can change depending on the context, nature, and perceived threat caused by the misuse of the personal information involved. The misconception of many organizations is that because privacy is largely a dormant issue for most people most of the time, the risk of not addressing privacy protections can be easily mitigated.

The problem in acting on this viewpoint was highlighted by an incident involving Human Resources Development Canada (HDRC), a federal government agency. In mid-2000, the "Longitudinal Labour Force File" caused an outrage among the public after it was revealed that this federal database contained personal information on virtually all adult Canadians. This included data collected from tax returns, child tax benefit payments, welfare files, federal job programs, job training and employment services, employment insurance files as well as the national health insurance master file—up to 2,000 pieces of information.

HRDC was subsequently deluged with negative reports by the media and numerous requests from members of the public to see their information. Despite the Human Resources Minister's original argument that this database "was essential for research purposes" and that “Canadians needn’t worry because it was secure,” HRDC ultimately deleted the computer program that enabled it to link its own information with data from Canada Customs and Revenue Agency within two weeks of the public learning of this database.

In his 1999–2000 Annual Report, the Privacy Commissioner of Canada expressed concern about HRDC’s approach to the management of policy analysis, research information and data with respect to this database. Issues raised in the Report included the File’s comprehensiveness, visibility, permanence, and the lack of a legal protective framework to govern its operation.

Actually, it “doesn’t take much for people to get really concerned about a particular company’s … privacy practices.”[13] Organizations cannot afford to assume that because a right is unexercised, it can be ignored or taken away.

[13] Jonathan Gaw, IDC Corp. March 29, 2001.

Proposed strategies for Information Security and Privacy Protection

As companies consider the security–privacy paradox and construct their privacy protection strategies, they will do well to remember the following factors.

Influences and Dilemmas

In the networked world of B2C and B2B, companies seeking to build trust must create end-to-end privacy practices that promise greater value to consumers. Following are examples of approaches that work—and some that do not.

- *What do customers really see?* At a time when trust is a major determinant of marketplace effectiveness, many companies are inadvertently creating a kind of "trust opacity" as they increasingly move towards technologies, such as self-service Web sites and automated voice response systems that inhibit consumers from having direct, personal contact with their representatives. The question becomes: If companies depersonalize the buying and customer care experience too much, will consumers have the confidence that their privacy and confidentiality concerns will be understood, much less resolved?

- *Catalyst for change*. The value of consumers' and business partners' personal information as business intellectual property is beginning to show up on balance sheets, triggering a host of accounting, tax, and shareholder value issues. How much is a market demographic database worth? How valuable is the raw data from which it has been developed? Who owns it? Where did it come from? Who else has access to it? What is its integrity? Can it be trusted? What is the nature and impact of the bottom line decisions based upon it?

- *Friend or foe?* New security approaches and technologies that monitor systems and networks—intrusion detection systems (IDS), incident response, and personal identification, authentication and authorization—all have the potential for being far more personally intrusive as they are tuned and strengthened to deal with more sophisticated and dangerous attacks. Cyber-terrorism has only increased this fundamental paradox. There is not and never will be a technology or policy that will bridge these points of conflict to everyone's satisfaction. The crucial point is that constituents of both viewpoints and their many variants maintain a co-operative and appreciative view of the others' requirements and pressure points. Fortunately, some important players in the information processing industry are addressing this issue. Continued dialogue and development are critical.

- *The value of a flexible approach.* Instead of trying to predict what the future may hold, companies should envision a number of possible future scenarios to guide their actions. With these future scenarios identified, they can develop flexible and modifiable privacy strategies by employing traditional planning models.

Forward-thinking companies are beginning to enable individually customized privacy approaches, where the exchange of value is tailored to the needs of each specific consumer model. To do this effectively, the enterprise must have a clear understanding of the concerns and priorities of its customers and business partners; few organizations do.

Strength and Risks in Numbers

As companies devise their privacy strategies, they will do well to remember that in many instances they will be in partnership with other organizations in the use and protection of personal information. Their strategy should encompass any entity that can have an impact, negative or positive, in this arena. Both organizations' practices must convey that promise through the entire "privacy-trust-brand" value progression. Of course, this is a two-way street. Both companies must support the other's approaches.

Where Companies Are—And How They Operate—Make a Difference

In October 1998, the EU declared privacy to be a fundamental human right.[14] And despite some ambiguity around the edges, what an EU business may or may not do with its consumers' personal information is quite clear. Personal information cannot be sold, rented or otherwise transferred to a third party without the individual's explicit permission.

In the UK, firms must comply with many forms of legislation when they seek to market their products and services directly. In addition to detailed provisions of the *Data Protection Act of 1998*, they must consider the requirements of other telecommunications regulations that restrict the use of public telecommunications systems for direct marketing by companies and individuals without specific consents. The UK is also implementing the eCommerce Directive, which will affect marketing via e-mail.

Italy, like other EU member states, forces firms to obtain informed and unambiguous consent—sometimes in writing—from individuals when personal data is to be used for direct marketing purposes, or is to be transferred to a country outside the EU. This requirement is onerous for companies conducting business online, where business economics and procedures often rely on having minimal written documentation. In practice, it means that Web site operators will not be able to use "cookies" to create individual marketing profiles without written consent—electronic consent is insufficient.

[14] "Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," The European Union, October 25, 1998.

Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), applies to the personal information of both customers and employees of banks, airlines, radio and TV stations, shipping lines, railways, or inter-provincial trucking companies, among others. Enacted in 2001, it also applies to organizations that disclose personal information across provincial or national borders for consideration. PIPEDA requires customer and client consent for the collection, use, and disclosure of personal information. Recent decisions by the federal Privacy Commissioner have focussed on the need for clear and unambiguous notice to customers about the uses of personal information. They have narrowed the circumstances under which an organization may rely on implied consent.[15] The federal law will apply to all commercial activities on January 1, 2004, if provinces have not enacted substantially similar legislation by that date.

The regulatory interventions found in Europe and Canada stand in sharp contrast to those in the United States. There, most uses of personal information by businesses are not only legal, but they are also part of daily commerce. Many U.S. industries, however, are worried about the unsettled nature of privacy laws. Various privacy initiatives are moving through Congress. States are free to adopt their own privacy standards. And internationally, U.S. firms that transfer customer and personnel data out of Europe must comply with European privacy laws. Some U.S. firms have adopted as their global business rule the European privacy standard, which is gradually being followed by other countries. A handful have joined the Safe Harbor arrangement to allow personal information to flow between the U.S. and European countries. Rising to this higher EU standard creates uniformity and reduces potential compliance costs.

All of this is to say that companies with high public profiles are more likely to be susceptible to challenges, suits, and proposed regulation for privacy—perhaps part of the price of being global and successful.

Roadmap for Successful Strategies

Deloitte & Touche and the Office of the Information and Privacy Commissioner/Ontario believe that companies will achieve sustained success and cost effectiveness in information security and privacy protection by developing flexible strategies. Flexible means adapting fundamental principles, standards, and technologies to your own environment and priorities. It also means treating this approach as an ongoing process, requiring review, fine-tuning, update, and, in some cases, major reconstruction.

[15] For a review of the latest findings of the federal Privacy Commissioner please see: http://www.privcom.gc.ca/cf-dc/index2_e.asp.

The following steps outline our recommended approach. In it, security and privacy reside together in order to help you determine where effective combination of effort and expense can take place. The diagram that appears early in this paper may also be helpful. You may have already initiated many of these steps and programs. But for clarity and continuity, we present the following as if you are initiating a program for the first time.

1. Identify, at a high level, the complete range of players and the information resources in use by both your organization and your processing partners. Too much detail in this procedure can consume unnecessary time and resources. But remember that many sensitive items may be outside of your organization's perimeter, yet still within your business responsibility. This work is best organized around business processes rather than by organization or technology platform, so follow the information process.

2. Categorize the information resources as being either *personally identifiable* or *not*. This may be challenging, especially in composite or embedded files. Also consider the services that support you, but do not transfer their files to you. You may have liability for their content.

3. Within the two categories, further segment each group by level of importance to your organization. A formal classification scheme for both security and privacy will add greater clarity and consistency to this program.

4. Identify those resources that have both important security and personal privacy characteristics, such as credit ratings, market preferences, medical records, net worth, and the like. These require special analysis to determine whether a potential conflict exists between the security needs of the enterprise and compliance with privacy protection regulations and standards.

5. Identify all business and technological locations of these information resources. Do not make hasty assumptions, and remember your partnerships.

6. Now draw a linkage between this "classified" information to the information systems supporting them, as well as the management responsible for its use and disposition. Thus far, we have not mentioned legal, audit, security staff, or privacy specialists, although they are major participants in the analysis outlined above. The objective, at this stage, is to establish the business context and requirements first and then work back to a technology, compliance, and information retention context. The clear implication is that these groups are support entities that will carry a major load, but are not the responsible "owners" of the information-supported processes. Too many enterprises only involve the business management incidentally in the decision-making processes. Too few business managers have a clear understanding of their direct responsibilities. The result: privacy protection fog.

7. Now you can begin to design a technical, management, compliance, awareness, and external relations program surrounding both security and privacy. Bear in mind that your security techniques—access management, encryption, audit trail, monitoring, incident response, and a score of others—must be validated not only for their effectiveness in protecting intellectual property, but also as to whether they support or inhibit your privacy efforts.

8. Your first design efforts should address the functions to be performed, not who will perform them. Jumping too early to judgment on departmental responsibilities can warp the design that will later be modified to deal with the realities of your organization.

9. Evaluate the program against current regulations, company policies, and perceived best practices. Include your processing partners.

10. Compare the proposed program to your current status in terms of actual practices and functions performed. Identify any gaps, conflicts, and overlaps.

11. Examine your organization and specialty staffing. Is there a fit? Is the staff adequate? Does the corporate culture support what needs to be done? What are the feasible roles for business management?

12. Reality time. Size up the effort required and make adjustments and trade-offs. The totality of the desired design will seldom be feasible in the first stages.

13. Create a timeline for development. Pick projects that will create immediate results and long-range benefits. When regulatory compliance is a dominant force, resist the effort to concentrate exclusively on those elements. You may paint yourself into a corner.

14. Formally report to senior management and solicit approval. Progress reports to management throughout the process are critical to ensure continued support and to eliminate the surprise factor. The final report should contain no surprises.

15. Assuming full or partial approval, you can begin to formalize and publish policies, procedures, and standards. During the design process, these have been evolving. They will continue to evolve throughout the life of the enterprise and should be reviewed periodically for currency and applicability.

16. Initiate the technology, organization, awareness, publicity, measurement, and compliance programs required. Make sure you have an adequate evaluation program to determine both progress and commitment to the design.

Many of the above steps represent significant efforts. Such a program may take years to establish. But this program, like other critical transformation efforts, is a continuous process and must be designed, planned, and managed as such. Yet when properly executed, the program can generate benefits very early in the development cycle.

For further information, contact:

Brian Beamish
Director of Policy and Compliance
Office of the Information and Privacy Commissioner/Ontario
Toronto, Ontario M5S 2V1
1-800-387-0073
info@ipc.on.ca

or

William Levant
Global Privacy Practice Leader
Deloitte & Touche
Two World Financial Center
New York, New York 10281-1414
212-436-2172
wlevant@deloitte.com

Robert Parker
Partner
Deloitte & Touche
79 Wellington St W. Suite 1900
Toronto, Ontario M5K1B9
416-601-5927
rparker@deloitte.ca

Rena Mears
Partner
Deloitte & Touche
50 Fremont St Ste 3100
San Francisco, California 94105-2230
415-783-5662
renamears@deloitte.com

Information and Privacy Commissioner/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

Deloitte & Touche
181 Bay Street
Bay Wellington Tower – BCE Place, Suite 1400
Toronto, Ontario, Canada M5J 2V1
416-601-6150
Fax: 416-601-6151
Website: www.deloitte.ca