8

Privacy and Information Technology Security: International Trends

'The concept of human rights and privacy legislation in our liberal democracies has grown over the past two centuries and most of this came to fruition in the 20th century. Privacy is now understood to be a human right. Individuals have certain expectations regarding how they are dealt with in our society, one of these being the understanding that certain aspects of their lives are sacrosanct and only shared in cases of justifiable legal requirements'.
Thomas B. Riley, *Security and Privacy: Striking the Balance*[1] .

Introduction

One of the most enduring policy issues is privacy. In the development of e-government practices and principles over the years, privacy and security have become key factors to ensure the success of online programmes. Both of these are important issues, due to the changing nature of technologies and the way people react and use these technologies. From an e-government perspective in government, new technologies are invaluable in connecting with citizens. However, privacy is an important value and in surveys on e-government implementation, the issue arises of people wanting assurances that their personal information is secure. Beyond privacy, there are also security issues on a broader scale, with the rise in 'spam', 'spyware', 'ad-aware', 'phishing', identity fraud and a host of other hacker activities (good or bad) that make people uneasy when going online. Governments who have evolved e-government and digital strategies have put a lot of emphasis on the importance of security, and on ensuring that secure networks are viable.

E-government is growing at a rapid rate around the world. At the time of writing it was estimated that 94 per cent of countries in the world had some form of online services. The degree of e-government programmes varies greatly from country to country. However, it is clear that with e-government online services there is a need to ensure that a whole series of policy measures are needed. As noted above, essential policies for good governance are privacy laws and security measures to protect individuals who go online to take advantage of online government programmes and services. Privacy and security are essential to ensure the growth of e-government. This chapter deals with the issues surrounding privacy, which include the security of information and data online and offline. Another central issue dealt with in this section is the importance of

technologies that enhance online privacy and ensure that individuals' personal privacy is protected.

Privacy is important in the minds of individuals and a lack of privacy or security, and the possibility that an individual's personal information might be used for illicit purposes, can have deleterious effects on an e-government programme. In a democracy, technologies that inhibit or potentially erode privacy then becomes another important social and legal issue; this is explored further in this chapter.

Privacy as a human value: why privacy?

> 'The personal life of every individual is based on secrecy, and perhaps it is partly for that reason that civilised man is so nervously anxious that personal privacy should be respected'.
> Anton Chekhov

In many countries of the world, privacy has come to be cherished in recent decades as an invaluable and inalienable human right, inherent to a free and democratic society. Privacy legislation endows the individual with certain rights and responsibilities, and establishes rules and guidelines for the ways in which public and private sector organisations are allowed to handle the personal information collected on individuals and groups in society. Such laws protect the individual from intrusion into their private lives. Individuals have the expectation that many areas of their lives should be shielded from the prying eyes of governments and the public. As such, only those people with whom they want to share their personal lives and their personal information should be privy to those areas of their lives.

The emergence of information technologies for marketing and other purposes is creating concerns for online citizens around the world. During the past two decades, people have come to understand the real threat of having their personal information accessed illegally online. Information technologies now have the capacity to not only collect vast amounts of identifiable information on citizens around the world, but are also able to automatically pick up information from websites. In addition, computers have programmes that look for certain types of information and automatically pass it on to other computers. Marketing techniques, meanwhile, have become increasingly sophisticated. This has led to demands by citizens for improved privacy protection. The following section provides some background on why privacy provisions are essential when information is used (or abused) on a network or in databases. It should be noted that there is a distinction between the use of personal information and public or non-identifiable information.

Endemic to all privacy laws are a set of fair information practices that set the boundaries for protection of the individual, while at the same time allowing a certain latitude for organisations to use personal information when necessary and allowed by law. Privacy laws, those who administer them and a public who values privacy and speaks out against potential abuses of these laws, are all essential. Privacy laws are the walls

that protect individuals against a possibly intrusive society. These laws have acted as the barriers against intrusiveness and have met, to some degree, expectations of protection. In a society of growing surveillance, the walls between the private and the public are beginning to crumble. More and more organisations, governments included, know more about individuals than ever before in history.

In the United States, there is a Federal Privacy Act. All 50 states in the Union have some form of a privacy law. It is the same in Canada, which has a Privacy Act (1982) in place at the federal level and where all ten provinces and three territories have some form of privacy legislation. The United Kingdom, Australia and New Zealand follow the same course. There are now numerous national privacy or 'data protection' (the European designation for 'privacy') laws around the world. These laws are prevalent in North America, Europe, New Zealand and Australia, with many other countries following suit.

The European Union Directive on Data Protection requires that all 27 member countries to have data protection (privacy) laws as a prerequisite to be a member of the Union. These laws are universal in their coverage, dealing with both the public and the private sectors. The Fair Information Principles set out in the Directive are to be enshrined in all the laws enacted by the member countries. One of the clauses found in the Directive states that a member country might prohibit the flow of personal information to another country if the latter does not have an adequate level of privacy protection. This means that individual countries can prohibit the flow of personal information to another country if it is judged that the country to which the information is being sent does not have sufficient privacy protection.

There is also the Council of Europe's Convention on the Protection of Personal Information (1982) and the OECD Guideline's on the Protection of Data (1980). These instruments were originally developed in response to concerns about automated information and its power to harm the individual. However, the European Union Directive mandates that both automated and manual files are protected. Europeans see privacy as a human rights issue. Many might argue that it is a non-tariff trade barrier, as it could restrict trade practices by disallowing the sending of personal information to other countries without laws and policies to adequately protect such information. However, the essence of all data protection and privacy laws is to protect the individual from having his or her information misused or abused. This has in it elements of making organisations accountable for what they do with personal information which they collect, while also endowing certain rights on the individual who provides the information. The European Commission Directive on Data Protection, in its preamble, stresses that this is a human rights initiative.

Appendix 1, below, sets out the essential governing principles in the European Union's Directive on Data Protection[2] .

The following section details the 'Fair Information Practices' recognised in all data protection and privacy laws around the world.

Fair Information Practices

All international conventions, laws, guidelines and policies, essentially incorporate three basic privacy principles, that is:

1. The individual has the right to inspect his or her own files kept by an organisation
2. Specific administrative principles setting out the collection, storage and dissemination of information; these principles lay out:
    a. how the information shall be collected;
    b. how long it shall be stored before being destroyed (usually only seven years);
    c. that the information is kept secure and only accessed by authorised users;
    d. what the limitations shall be on sharing the information with others;
    e. the necessity to use the information only for the purpose for which it was gathered;
    f. that the consent of the individual must be gained if the data is to be used for another purpose;
    g. the right of the individual to have access to the file (in whatever form) containing the information, to determine its contents and veracity;
    h. the right to have false, misleading or erroneous information in the file either deleted or corrected;
    i. the right to make a notification in the file if the information is not corrected or deleted; and, under the final principle,
3. The individual shall have the right of appeal to a body independent of government, if the individual believes one of the principles have been violated.

One of the more important functions of privacy officials is informing individuals of their rights under the respective laws and identifying emerging trends and issues in society posing privacy threats.

What is all this concern about privacy? What does this mean to cultures where the concept of privacy is very different? Databases created by public or private sector organisations are usually subject to criticism if they in any way contain personal information. Thus, it is important to assess why people are concerned about possible abuses of their personal information. It is also important to set out how easy it is to collect identifiable information in today's technological environment.

The following section provides an assessment of the issues and possible solutions regarding privacy and the online technologies. Government agencies can develop security technology mechanisms for individuals and groups to protect their privacy online.

Issues arising

The main features regarding privacy laws and citizens are as follows:

- All citizens where countries have privacy legislation have equal privacy rights.
- There are now billions of pieces of information in thousands of databases, floating around the Internet.
- Individuals are increasingly appearing on websites, such as YouTube, MySpace and Facebook, and are liberally sharing their personal details online.
- 'Cookie' technology can track a person's behaviour and preferences, and computers can now be programmed to 'talk' to each other.
- Private sector organisations are using personal information increasingly to market products, services and goods, but are not necessarily getting informed consent from individuals to use their personal information.
- Citizens want the right to be able to consent to the use of their own personal information.
- There is a rising awareness among many citizens of the need for deeper protections of their personal information, i.e. taking responsible action to protect one's own personal information when possible.
- While there are currently many data protection/privacy laws in place, measures are still needed to assure citizens that their personal information is not being abused.
- Educational measures from offices of privacy commissioners and data protection registrars/commissioners contribute to raising privacy awareness amongst the public.

The basic premise of privacy

Privacy plays an important part for governments in the development of online services and the implementation of new technologies. For example, the Canadian Federal Privacy Commissioner has commented on how the rise of new technologies presents an ever-growing threat to essential freedoms[3]. Privacy and data protection commissioners around the world often comment on the impacts of new technologies and how amendments to current acts, policies and applications are needed to guard the privacy of individuals. Privacy commissioners also provide advice and solutions online on their websites on how individuals can protect their individual privacy, both on the Internet and when dealing with corporate, commercial and other organisations who collect their personal information[4].

Many privacy commissioners and academic scholars see loss of privacy through the intrusiveness of surveillance technologies as concomitant to the threat of the loss of hard won freedoms. The argument is that perhaps not enough people yet realise that privacy and freedom are inextricably linked; one cannot exist without the other.... But

this failure to understand the link is pervasive and leads to many dubious notions taking root. Privacy and data protection commissioners run ongoing programmes that seek to educate the public on how to use privacy laws to gain access to their personal information, but also for people to understand the importance of an individual protecting his or her own personal information.

Addressing privacy and technology Issues

This section addresses the nature of privacy in relation to information technology and how technologies can be used to enhance privacy. It looks at different information technologies and how security, for privacy reasons, can and should be built into developing systems. It is important to understand that information technology security is only one small part of privacy, albeit an important one. However, because a site is secure or because there are security features within a smart card technology, for example, this does not mean that privacy standards are necessarily met. Security mechanisms are fundamental in ensuring universal privacy, and privacy laws need to reflect this fact[5].

The main issues in this respect are as follows:

- Information technology is neutral in its capabilities: it can be used to invade privacy or to protect it.
- Privacy protection requirements must be integrated into the development process, in the technical standards governing technology operation and within the general planning and architecture for systems.
- Concern for the vast amounts of personal information that are being collected by governments and by companies on the Internet.
- Meeting a balance between customer benefit and the need-to-know.

Technology and privacy: the importance of legislative protection

Privacy has over the past 20 years or more become a major issue internationally. The rise of intrusive technologies, the capacity of databases to store gigabytes of information and Internet advances have resulted in a surge in awareness about the importance of privacy. With respect to the Internet, a lot of pressure is being put on companies to develop privacy policies to protect consumers who are liberally sharing their personal information in this new environment. The rush by large corporations to engage in electronic commerce (e-commerce) over the past two decades, due to the growing dominance of technology in people's lives, has meant more personal information is being gathered, shared, sold and disseminated than ever before.

As noted above, many countries already have data protection (privacy) laws in place. The European Union has a Directive on the Protection of Personal Information that applies to all member states and guarantees that all citizens of the European Union have equal privacy rights. Hong Kong has a law in place that conforms to the

EU Directive. Malaysia has developed data protection standards in law. Canada's Privacy Act was passed by Parliament in 1982 and came into force in 1983. In 2001, Canada's Parliament passed the Protection of Personal Information and Electronic Documents Act (PIPEDA), covering private sector organizations and which came into force in January 2001. Part of Canada's strategy in developing an e-commerce policy was to ensure that laws exist to develop **trust and confidence** in individuals who come online to engage in electronic transactions. The United Kingdom also passed a Data Protection Law in 1983, which was amended in 1999 to meet the full requirements of the European Directive on Data Protection. The UK law is now harmonised with the Directive.

There is a Federal Privacy Act (1974) in the United States, but this law does not cover privacy in the private sector. The Office of Management and Budget, an arm of the Executive Office of the President, administers the Privacy Act by providing agencies with implementing assistance and guidance. However, there is no central agency or privacy commissioner within the United States Government charged with enforcing that law, nor with enforcing other privacy laws that govern private sector records, as discussed below[6]. Thus, the system in United States law for regulating privacy and handling privacy complaints from the public varies substantially from the majority of countries with data protection or privacy laws. For government records subject to the Privacy Act of 1974, the ultimate recourse for the individual is the Federal courts, although an internal administrative appeal to the agency maintaining the system of records is the first remedy[7].

Nonetheless, the Federal Trade Commission (FTC) is recognised as one of the key United States governmental agencies responsible for enforcing the wide range of federal privacy legislation that applies to private sector records, and it deals with a host of privacy issues and privacy violations that occur in that sector. A significant part of the FTC's mission is to educate consumers and businesses about 'the importance of personal information privacy, including the security of personal information. Under the FTC Act, the Commission guards against **unfairness and deception** by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information. Under the **Gramm-Leach-Bliley Act**, the Commission has implemented rules concerning **financial privacy** notices and the administrative, technical and physical **safeguarding** of personal information, and it aggressively enforces against **pretexting** (obtaining personal information under false pretenses). The Commission also protects consumer privacy under the **Fair Credit Reporting Act** and the **Children's Online Privacy Protection Act**.

The Department of Commerce has a programme called the Safe Harbor Program, which deals with the exchange of personal data from companies abroad. The Safe Harbor Program came about in the wake of the passage of the EU Directive on Data Protection. Given the scope of the data protection and privacy laws in Europe, i.e. their covering both public and private sector organisations, US corporations were concerned about the impacts these laws would have, for example, on subsidiaries in European countries being able to pass on personal information to their corporate headquarters

in America. The United States 'relies largely on a sectoral and self-regulatory, rather than legislative, approach to effective privacy protection, thus many US organisations were uncertain about the impact of the 'adequacy' standard on personal data transfers from the European Community to the United States'[8]. Thus, the Safe Harbor project was developed 'to enable US companies to satisfy the requirement under European Law that adequate protection be given to *Personal Information* transferred from the European Union to companies in the United States. The EU, which currently includes the 27 member states, has recognised the Safe Harbor principles, as have Iceland, Norway and Liechtenstein, as providing adequate data protection'[9]. The Department of Commerce interacts with the Federal Trade Commission on privacy issues in a global context[10].

All the privacy and data protection laws around the world seek to protect the personal information of the individual from abuse and misuse. Such protections have become increasingly important with developments in the online world and with the massive amounts of information being circulated every minute of every day.

The balance between service and privacy

Governments around the world, including United Kingdom government branches and departments, are increasingly gathering personal information from a variety of sources. Examples in the UK include the Department of Social Security, the police, and customs and immigration officials. Each will have sought permission from the Data Registrar's office for permission to match personal data from the different sources. Another major issue that has arisen over the last decade in the UK has been the implementation of CCTV cameras in every city and town in the country. At the time of writing there were an estimated 5.2 million CCTV cameras in the UK, monitoring citizens day and night. In the beginning there was a consensus from the public that this would help to protect people from crime. However, this attitude is changing as it is increasingly recognised that the proliferation of so many cameras is resulting in an intrusive surveillance society.

Unfortunately, this openness and ease of accessibility to personal information has been interpreted to mean that technology is inherently evil and an instrument of control of individuals. In fact, technology is not the problem; it is what governments, groups in the private sector and individuals overall do with personal information that is at the core of this issue.

The highly driven consumer of the early 21st century is both the consumer and the source of information. On the one hand he/she seems to want to protect it, on the other he/she is sharing it liberally. The answer to this is not necessarily stopping the sharing of information, but education as to how one's personal information is being used and can be abused to the detriment of the individual. This has led many technology experts and commentators to conclude that the price of technological convenience is an increasing loss of privacy. At the same time, others argue that technology is now

so pervasive in industrialised nations that privacy has been lost forever. Privacy advocates vociferously disagree with this latter view, arguing that **legislative standards** will handle the problem. Many ordinary citizens, not versed in the substantive issues surrounding privacy, know that there is a problem. Surveys indicate that more and more people want to see some mechanisms to protect their privacy in cyberspace[11].

It is recognised in privacy offices around the world that the rise of the Internet has brought with it new issues. One of these is how do you track or capture violations of the use of personal information in a networked society?

The technology impact on expectations

The transition from the 'Paper Age' to the 'Digital Age' has brought with it new issues for the collection, management and dissemination of information. In the past, especially prior to the rise of the personal computer, seamless international digital networks and the Internet, information was often difficult to retrieve. To access any kind of information often necessitated a laborious process. Now information from around the globe can be at one's fingertips: any curious citizen can browse the Internet, use search engines to find out whatever kind of information he/she is seeking from either websites or a multitude of other Internet-related sources.

However, there are serious downsides for people who use websites for a multitude of purposes and, unbeknownst to many of them, they are being tracked by companies. In response to these actions by companies, in November 2007, nine US privacy and consumer organisations asked the Federal Trade Commission to create a 'Do Not Track List'. The purpose of such a list would be to have restrictions placed on the tracking of personal information by companies to determine what kind of products an individual is interested in buying when they go to commercial websites. Companies collect such information in order to tailor their advertising messages. These groups want measures taken to enhance and protect the individual privacy of citizens[12].

Searches of public databases or websites can allow an individual obtain the personal information he/she wants, whether it is on themselves or another. Unless such personal information is specifically protected by statute or government policy, it can be easily obtained. Even those who are technologically literate cannot escape this net. An individual might not go online, but the information is still ending up in a database somewhere. Personal information is given out almost daily in our lives and the collectors of such information, whether a government agency or a private sector organisation, are storing it somewhere in some electronic format. It is almost commonplace now for people to register on websites and to be asked to give out some very substantive details such as name, date of birth, place of birth, home or business address and email address. If this information ends up in a commercial database, it can potentially be sold to other companies. This practice is now so widespread that privacy offices in many jurisdictions are developing papers and warnings of the dangers of providing personal information online. The message from such offices is for individuals to be careful how they provide their personal information. Many sites are secure and prevent attacks on

a site when an individual provides personal details. However, the bigger issue is to what degree commercial organisations are using the information for marketing purposes.

Activity on the global information infrastructure (GII) never ceases. For example, an individual can register on a website for a company in Canada. Another branch of the company might be in Australia. Within seconds that personal information can then be in the databanks of the Australian office. Something in a person's profile might make him/her a candidate for a certain product. A company selling that product might not only target the person, but can also sell his/her personal information to any other company in the world because of their profile. A person interested in skiing could have his/her personal information sold to travel agents, ski manufacturers, airlines, ski resorts or any industry related to skiing. There is no end to the infinite ways in which the information could be used. Personal information is spread out along the corridors of the world's integrated networks. If not protected by a statute barring access or use of it, it is there for the taking.

Thus, all citizens today are intricately intertwined within the global information technology and communication infrastructure, even if they do not use or own a computer or ever go online. Whatever transaction we engage in, whether it is using a bankcard to withdraw cash or fill out a form (and mail it) to join a book club, the information ends up in a computer. In the private sector this has proved a gold mine for marketers, direct mailing houses, researchers, private investigators and the just plain curious. Data warehouses are now common. Such 'data mining' is engaged in by large and small companies alike around the globe.

In the United Kingdom, the government passed the Regulation of Investigatory Powers Act (July 2000), which allows employers in both the public and private sectors to monitor employee emails. This illustrates the demands of government to pass legislation to handle a specific problem in the area of public interest versus the rights of the individual. There are therefore, many ways of obtaining information given the knowledge of the new information technologies, the right equipment and the expertise to use it. While few could even be bothered to get such information, there are many companies who want to know about personal and spending habits so that specific advertising of products can be marketed directly.

As shown above, web servers now have (and have had for a long time) the ability to customise a website on a person-by-person basis. However, imagine how hard it would be to keep the preferences for every browser that has ever visited Yahoo on a web server – such a thing would amount to billions of bytes of data. A much better way to do this is for each browser to keep his her own preferences: that is what 'cookies' do. Web browsers set aside a small amount of space on a person's hard drive to keep these preferences. Then every time he/she visits a website, their browser checks to see if there are any pre-defined preferences (cookies) for that server; if there are, it sends the cookie to the server along with the request for a web page.

This information can also be made available to other interested marketers. In other words, one computer is coded, for example, to respond to anyone interested in skiing. An individual comes in who is a recreational skier and indicates this on a site. That computer can thus be programmed and send this information to another computer in another company or country; the process can be continued ad infinitum. This makes the sources of personal information on individuals in cyberspace almost infinite. It also means that privacy has become almost non-existent. Nonetheless, privacy legislation when effectively applied can curtail such practices.

The problem with the cookie technology is when the behaviour of the individual becomes the subject of profiling and the information collected is put up for sale on the Internet. Individuals can erase these cookies from their computers, but many are not aware they have the capacity to do this. Erasure of cookies prevents any future tracking next time a person goes back to a site, and gives a choice as to whether or not the individual wants to exercise his/her privacy. However, the privacy issue moves far beyond protecting personal information on the Internet. In a larger sense, privacy is being violated daily as new and all encompassing surveillance technologies come on the market.

A large majority of the citizens shopping online want to ensure that their personal information is protected, secure and confidential. When surveyed, the public asserts strongly of their fear of privacy invasion in our new technological environments. At the same time, many of these same people freely use the new technologies that are slowly eroding freedoms. With each use of these technologies, without debating the long-term deleterious effects on society, individuals are creating an ever-tightening electronic noose around society's collective neck. There are many examples of how technology is being used to snoop into our lives. From the cameras in the corner shop and in every shopping mall to the ever-increasing emergence of personal smart card technologies, being developed by the public and private sector alike, millions of bytes of personal information are going into databases. People are increasingly accepting what was once considered inappropriate and unacceptable.

Citizens often willingly give up information so they can receive some benefit in return. Global positioning system (GPS) technology has had the capacity for years to send email, faxes and text messages to pagers, blackberries and personal digital assistants (PDAs) and, now, even to cars. But that same technology can also pinpoint exactly where a person is at any given time of the day. Employers can monitor every aspect of employees' movements through these technologies.

The Ontario government in Canada in 2001 had planned to develop smart cards that would combine a citizen's driver's license, health card, birth certificates and fishing licences. However, by 2003 the government had deleted the project because of citizens' concerns that the card would have contained the individual's unique fingerprint. The problem with such technologies is that privacy laws cannot adequately protect the citizen. In time, such unique identifiers can be expanded for usage by more and more government agencies. Soon this could become a card that citizens would have to pro-

duce on demand. To refuse to do so could tag the citizen as having possibly something to hide. The personal information could still be protected by a privacy act, but such protection cannot guard against the human consequences.

It is becoming clear that people are concerned about how their personal information is bandied about and traded. People sense that the issue here is greater than privacy. The developed world is witnessing the development of two separate identities for every individual: the real person as perceived in the physical world by family, friends, colleagues etc., and the virtual self growing in cyberspace and held in databanks around the globe. The latter (data shadows) is based on real data that is, in itself, subjective and not necessarily reflective of our true selves.

The proof of this can be found by simply going to MySpace.com or Facebook.com where individuals download pictures and information about themselves. Some people are anonymous, but the majority are under 25 and happily provide such information. These are effective communication tools through which friends and acquaintances cam communicate, share stories or ideas and meet new people. This new generation involved in this social networking are the post-modern babies born in the 1980s; they have adapted seamlessly to these new technologies.

People are now raising fears that this makes individuals subject to decisions being made by the 'invisible controllers' of this infrastructure. People are becoming intuitively worried about the forces driving these technological developments (including the negative acts and anti-social behaviour of a minority online). Fears about loss of privacy actually reflect a deeper fear of what technology is doing to people as individuals. Often information issues such as privacy are seen as an impediment to technological development. Many believe individual rights have been parked to the side for these 'greater' interests.

Under Canada's privacy law, the Federal Privacy Commissioner has the mandate to educate Canadians about their privacy rights[13]. It is through forums, such as in the Annual Reports of privacy commissioners around the world and educational programmes, that people's awareness will be raised of the need to strike a balance between the development and usage of new technologies and potential threats to freedoms. Armed with knowledge, people can make informed decisions.

On a wider, international scale it is becoming essential that privacy be enacted as a human right and that laws be developed and implemented throughout the world. Some 94 per cent of countries have online programmes, but far fewer have privacy or data protection laws. A broad right is needed that is not only enshrined in law, but will create a culture around privacy as a human right. Europeans recognise that privacy as a human right is implicit in their laws. Some form of international convention on privacy as a basic human right is needed. Privacy and Data Protection Commissioners are also proposing the development and implementation of International Privacy Standards worldwide.

Privacy, information technology and security

Privacy and technology are linked in the public's mind. It must be recognised, however, that current and emerging information technologies are vital to how public organisations will have to operate in the Information Age. It is impossible to adopt the 'Luddite' approach that all technology is *ipso facto* 'bad for us' and must be avoided at all costs. The social service state that exists in most developed countries, with the strong demand from citizens for services and entitlements, also creates a need for such technologies. Thus what emerges as a more likely objective within public administration is a balanced system of privacy protection that:

- limits the amount of personal information collected to the absolute minimum required for programme operation and service delivery;
- employs technology to support anonymous transactions, whenever this is possible; and
- applies technology to personal information systems under a strict code of fair information practices[14], which are the basic guiding principles of all privacy and data protection laws worldwide.

As has been mentioned before, information technology is neutral in its capabilities: it can be used to invade personal privacy or to protect it. The key is the intent of the organisations in applying it. There is a tremendous expectation on the part of the citizenry in the developed world that governments and public agencies will act in ways that both enhances programmes and services and better protects personal privacy. Thus, it is fair to say that technologies normally follow programme directions and it is public policy, as much as technology, that needs to be influenced from a privacy protection perspective. However, it is important to understand the technology and how it can influence privacy protection for both good and ill.

Electronic networking

Distributed networks or computing is the current modern wave of pervasive information technology. The international symbol of this is the **Internet**, a 'network of networks'. But networks come in many more modest forms. A programme or a public body may have an enterprise-wide network which carries email, major databases, exchanges work files and controls administrative work (forms, budgets etc.). Corporate 'intranets' developing within many public organisations and across governments are a type of enterprise-wide network for the government, as are common personnel systems based on different software, and any attempt at government-wide email services. There are also growing numbers of social networks, such as MySpace, YouTube and Facebook. Millions of people, especially teenagers and young adults, thrive in this online world and interact with friends locally, nationally and internationally.

Most public bodies and governments are working on better government-wide computing and communications infrastructures to enable the wide sharing and exchange of information. Other examples of this type of network are property registries

and distributed service delivery systems, such as employment databases with interactive service, used in many countries, such as the UK. Such database applications are immensely popular with public sector administrators.

Another type of network is one maintained by one programme, but which has multiple interactive uses by several other programmes or public bodies. A motor vehicle registry is an example of this type of network. This could be the Internet or a host of more specialised databases. This poses a serious security problem, because these communication links can be targeted as a weak point in penetrating government systems, and the databases themselves can become unauthorised sources for collecting personal information.

Networks can be the source of a myriad of privacy protection problems, such as:

- their being the source of unauthorised collection of personal information;
- through incomplete partitioning of network modules and insufficient access and authentication controls, being the source of unauthorised access to and use of personal information;
- where there is multiple use of a network and lack of accountability as to who is using what information and for what purposes, and lack of control over disclosures of information;
- where networks permit many sources to update files, concerns for the completeness and accuracy of information; and
- major security pressure points, such as access and authentication controls, communication security and external access firewalls.

Well-chosen software can provide access control, encryption, network management, audit controls, logging, labelling, isolating of sensitive data, system recover, and integrity verification techniques, all of which support privacy protection. Poorly chosen software can be manipulated to permit bypassing or over-riding of system controls, and thus permits personal information to be used or disclosed in unauthorised ways. It can also be used to modify data or make systems work in unauthorised ways. Organisations need to assure themselves that there are design and implementation standards being employed that address these privacy problems for both current systems and in the modification and establishment of computer networks.

Some of the above points might be addressed by integrating privacy protection needs into the general planning and architecture for system development and into the technical standards governing technology operation within an agency. This could be achieved in the following possible way:

For hardware:

- the configuration of equipment to meet privacy goals;
- maintenance of a configuration chart;

- identification and use of security features implemented within hardware;
- authorisation, documentation and control of changes to the hardware; and
- authorised processes for maintaining of IT equipment.

For software:

- administrative controls, including segregation of duties of information technology;
- staff, maintenance of an inventory of authorised use and security reviews of this;
- development of software life-cycle standards, including design, development and test;
- standards and surveillance;
- change control and problem resolution;
- quality assurance;
- configuration management;
- identification and authentication;
- isolation, encryption and access control; and
- audit controls.

Communications:

- procedures, practices and equipment for protecting the electronic communication of personal information.

There is a wide variety of cards that can be used for identification and transactions for government programmes. The most common are embossed plastic cards that identify individuals through information on the card, such as name, address, account or license number, photograph and other identifying characteristics. In such instances, the card itself is the record and, short of adding more information to the face of the card, it is relatively static in nature. Such cards have been employed in government programmes since the 1940s.

Another type of card, now increasingly common in government, is the magnetic strip card introduced by credit card companies in the 1970s. The most common card of this type stores up to 240 characters of information. The stripe has three tracks, each used to store information for different applications. One of the tracks is designated a read/write track and, with appropriate terminal equipment, can be updated. Such cards are popular with business and government because production costs are low and international standards apply to the cards. There are, however, drawbacks to such systems: the magnetic stripe can easily become damaged; the cards are relatively easily counterfeited; and they are restricted to one use.

Magnetic stripe cards can be used with a personal identification number (PIN) to aid in authenticating a user (e.g. an automated teller card), but such cards are not a good medium for sensitive data because of the high risk of unauthorised access.

There are also memory cards that have microchip or integrated circuits, with fixed memory functions, but no intelligence or processing power. This technology has led to the optical or laser card, which replicates an optical disc on a miniaturised scale. Information is written onto the card using a laser and can be retrieved using special reading equipment. Such cards can store 1,200 plus pages of text and operate on the WORM ('write once read many') principle. It is possible in such cards to establish file systems and access controls to these, security – including encryption – being provided through the reading device rather than through any software on the card itself. The advantages of the card are its high memory capacity, relatively low cost (on account that the card has no processing power) and higher durability to electrostatic or magnetic damage.

In the last decade, in North America the technology commonly known as 'smart cards' has become the latest generation of transaction cards. A smart card resembles a conventional bank or credit card, but it contains an integrated circuit chip. The chip embedded in the card can process and store data. Each card is supposed to be able to support multiple applications, and each of these can be secured from the others. For increased security and data integrity, the card is usually capable of encrypting data to be stored on it, or data that are to be transmitted to a host computer. There is little agreement on any internationally recognised definition of a 'smart card.'

The latest 'smart card' to be developed contains complete data sets on an individual, but is also controlled by the individual. Thus, an individual could have a photo ID card with an embedded chip in the card. The chip could contain a wide variety of information, but the information could only be accessed through the consent of the individual. The individual would insert this card into a reader, for example, in a government agency seeking information. Only the individual would have the password to the card and thus could control who has access to the information. This is seen as a potential all-purpose card for the individual. Thus such a card would satisfy a variety of interests pertinent to the administration of government services and benefits for the individual, while the individual would continue to have control over who sees his/her personal information.

In addition to password and access controls, a 'smart card' can carry out authentication procedures. This means that it can identify all parties involved in a transaction, and determine if they are authorised and/or authentic users. This can be done through a log-on procedure that requires particular information either unique to or only known to the authorised user.

Finally, information on a 'smart card' can be encrypted to protect information from unauthorised access and to certify or authenticate particular transactions.

The following are some of the features and privacy principles that 'smart cards' should contain:

- the implementation and ongoing use of ID cards should conform to **fair information practices**;
- there should be **full transparency** in the implementation and ongoing use of ID cards;
- the principle of finality (i.e. all uses of ID cards must be decided in advance) must be applied to the conception and implementation of ID cards;
- the use of ID cards by the public should be voluntary, meaning that they should be used by informed consent only;
- ID cards should in fact be **smart cards**, where the individual alone can control the use of his/her card, including authorisation for its use by means of a unique password;
- individuals must be able to control access to their own data;
- there should be a **prohibition on the routine profiling of individuals** based on transactional data, unless there is reasonable and probable cause to do so for law enforcement purposes;
- there should be **oversight, audit and complaint-handling mechanisms in place for ID cards**; and
- the holder of an ID card should be identified by his or her **digitised photograph, rather than by a unique personal identifier.**

Encryption

Encryption is a process that transforms clear text into unintelligible form. Ciphers have been used for centuries to protect both military and business correspondence of a secret or sensitive nature. Encryption, as applied to electronic communications, is looked upon as one of the prime ways, along with digital signatures and authentication devices, to protect the privacy of individuals in a networked world.

The two main types of encryption are symmetric cryptosystems and public key cryptosystems. In symmetric systems, one common key (an extremely large number) is shared by both parties for encrypting and decrypting messages. Each party must know the key. However, such systems as the Data Encryption Standard (DES) described below, are relatively fast and provide good protection for bulk transmissions of data. DES is a hardware-based technology.

A public key system uses two different keys – one public and widely distributed and the other private and secret to the person encrypting the message. What is encrypted with one key may only be decrypted with the corresponding other key in the pair. Such systems are slower than symmetric systems and also require considerable attention to

the key management process, especially when the users are outside a closed system and on an open network[15].

The essential and core enabling technologies are described here because they relate to the application of encryption measures. They are as follows:

- A **public key infrastructure (PKI)**. Public key cryptography will be the enabling technology for securing personal information and other information from unauthorised use and disclosure and to assure authentication of documentation by digital signatures just as hand-written signatures verify paper communication. Enabling legislation for PKI has been passed, in 1999 and 2000, in Canada, the US, the UK and Australia with many other countries following suite. Governments recognise the need for both a PKI and a mandate of authority for some type of common service organisation or organisations to serve as the public key authorities. These authorities will manage the key structures in a uniform way and assure the key certification process to ensure that the PKI is effective. PKI is the infrastructure that integrates other technologies, such as electronic authorisation and 'smart cards', into a seamless solution for secure information management by a public body.
- **Electronic authorisation and authentication (EAA)**. This is a set of information technology services that, when combined with management practices, results in electronically implemented accountability controls that may be used to enable management to exercise due care in the conduct of operations and programmes. EAA services are needed to enable managers to maintain accountability in an electronic programme environment. These services are needed to ensure authenticity and the integrity of information transmitted electronically, and to allow the authorisation of electronic documents. In essence, electronic means are needed to implement controls, including privacy protection measures that are commonly provided and generally applied in the paper environment.

In summary, there are major challenges to applying encryption techniques to large distributed information technology systems. Nevertheless, such applications hold the major promise of providing the security protection required in a networked world. These applications provide both privacy protection and promote the growth of electronic commerce, thus those challenges need to be met head on. Law enforcement and security agencies in both the United States and Canada are concerned that they are losing control of the encryption field to business and other operators that will build encryption codes that cannot be broken. As well, the encryption field is one that is controlled by standards and strict import/export regulations (most American encryption information cannot be exported for use outside North America). There also remains a problem with many encryption devices: they remain awkward to use and slow down reaction time on networks substantially.

Given these constraints, encryption should be considered for application only where there is sensitive personal information on a system and it must be communicated electronically (e.g. by modem or fax) or the application itself (e.g. a 'smart card') is

sensitive and demands superior security measures be built into the system. However, having stated these cautions, PKI is destined to become a major privacy and security technology for distributed network systems. Consequently, it is important that the government as a whole has a strategy and action plan for dealing with these developments when implementing new projects. Most encryption devices are bought from lists of trusted equipment approved by national security agencies. Some, however, are from organisations that work with agencies for non-classified encryption measures and their software is installed and configured by experts in communications security.

Conclusion

The rise and spread of information technologies, new security laws and the pervasive influence the network of networks, the Internet, is now having on society are raising deep concerns in society about the possible abuses of these technologies, by public and private sector organisations alike. An analysis of the capacities of the new technologies to be able to collect, assuage, disseminate and exchange information is essential in order to provide strong privacy protections.

It is clear that privacy is an abiding issue in democratic and developing societies and will continue to be over the decades to come. That is why it is important that organisations in the public and private sectors ensure there is a clear privacy statement on their online websites.

Recommendations

In general, governments in the Caribbean countries need to develop a clear data-matching policy that lays out consistent and clear rules as to whether or not any form of data matching is allowed. If data matching is to be allowed, in limited circumstances, then specific limiting principles need to be set down.

It is also recommended that countries engage in an ongoing debate on privacy issues, and ensure that appropriate privacy and data protection legislation is put in place. Educating the public is a good start, with many countries running extensive educational campaigns. These include:

- National television advertisements;
- Booklets, describing how a country's legislation works and a primer on how the citizen can apply for their personal information in public or private sector organisations. These booklets are distributed in public places, schools and offices around the country;
- Officials of the Data Registrar's office speaking at public events to inform people of their rights; and

A toll free line people can call to reach officials of Offices of the Data Commissioner's and Privacy Commissioners Offices once such offices are created.

Notes

1. Riley (circa 2003), available at: http://www.rileyis.com/publications/index.html [accessed 5 February 2008]
2. Official title of EU Directive: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
3. Office of the Privacy Commissioner of Canada, available at: http://www.privcom.gc.ca/keyIssues/index_e.asp [accessed 5 February 2008]
4. For two examples of how privacy commissioners educate people on protecting themselves online see: Canada's Federal Privacy Commissioner, available at: http://www.privcom.gc.ca/ind/index_e.asp [accessed 5 February 2008]; and United Kingdom, Information Commissioner responsible for Data Protection Act, available at: http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx [accessed 5 February 2008]
5. Cavoukian and Tapscott (1995).
6. Furthermore, the Privacy Act of 1974, as a purely federal law, does not protect the privacy of records maintained by state governments, many of which have adopted their own versions of the federal law.
7. See Federal Trade Commission Website, available at: http://www.ftc.gov/ftc/privacy.htm [accessed 5 February 2008]
8. Privacy Act of 1974, as amended, 5 U.S.C. 552a, available at: http://www.usdoj.gov/oip/privstat.htm [accessed 5 February 2008]
9. Department of Commerce Letter to Industry representative, 8 November 1998. Available at: http://www.ita.doc.gov/td/ecom/aaron114.html#Safe [accessed 5 February 2008]
10. See: http://www.techteam.com/Investors/PrivacyPolicy-SafeHarbor04-05.pdf [accessed 5 February 2008]. Full details of the Safe Harbor Principles and Privacy policy can be found at http://www.export.gov/safeharbor/ [accessed 5 February 2008]
11. Rotenburg and Agre (1997).
12. This proposal was made to the Federal Trade Commission on 1 November 2007. As of this writing, no regulations had been put in pace to curtail the practice of web monitoring by companies when individuals went to websites.
13. Many countries around the world carry out extensive public relations programmes to make citizens aware of their privacy rights. The degree of such education is dependent on the size of the offices and financial resources.
14. See above section on Fair Information Practices.
15. Schneier (1994) and Cavoukian and Tapscott (1995).