ELECTRONIC GOVERNMENT (1999)

E. Michael Power[*]

Introduction

The popularity of the Internet has triggered capacity growth and, in turn, has provided an incentive to shift from expensive, dedicated private networks to the public, open Internet in order to exchange information and conduct business. The exploitation of the Internet for "electronic commerce" has become a popular topic in the course of the last year. The idea of governments using electronic means to do what governments "do" is a logical extension of the general trend in society today.

Why are governments only now beginning to address the subject? We generally seem to forget that World Wide Web is "only" five years old which is not a long time given the impact that the Web and the Internet has had on society. Not only do governments have to address the subject but they — being governments — have to get it right. Various initiatives indicate that governments at all levels are increasing their use of electronic means to do business.

The activities of government with respect to the Internet can be characterized in two ways. The first is facilitating the use of the Internet as a medium for communications and commerce. The second is to be a model user to build trust and confidence in particular communication technologies. Attaining the first objective can be done by ensuring that the legislative and policy framework is in place to encourage or, at least, to not inhibit the use of electronic media. Being a model user means developing the technical infrastructure and re-designing government service/business processes in the creation of electronic alternatives to existing methods. This paper will describe some of the federal government's activities in changing the legal and policy framework and in becoming a model user of technology.

[*] Department of Justice Canada, currently seconded to Treasury Board Secretariat serving as Assistant Director, Policy, Interdepartmental PKI Task Force. The views expressed in this paper are personal and do not necessarily reflect the views of the Department of Justice, Treasury Board Secretariat or any other department or agency of the Government of Canada.

Canadian Electronic Commerce Strategy

The Prime Minister outlined the elements of Canada's Electronic Commerce Strategy in a speech made in St. John's Newfoundland on 22 September 1998.

> Many countries are developing strategies to meet some of the challenges of electronic commerce. But Canada is taking on all of them. Our bold and comprehensive vision will make it possible for Canadian business and consumers to seize the potential of E-com first, and fastest.
>
> We call our E-com strategy "The Seven Firsts". And most of it will be in place by the end of this year.
>
> - We will have privacy legislation to protect personal data.
> - A policy on the use of encryption technology.
> - And a world-class public key infrastructure in place.
> - New consumer protection guidelines will ensure that Canadians enjoy the same protection online that they do at the corner store.
> - We will table legislation that gives electronic signatures a basis in law.
> - A revenue neutral taxation regime will ensure that you are not taxed twice.
> - And we will have standards that the world will follow.

Federal legislative and policy initiatives are targeted to meet these "deliverables".

Cryptography Policy

The protection afforded by applications using public key cryptography depends on such things as algorithms and key lengths. This is commonly referred to as the "strength" of the cryptography. The stronger the cryptography the less likely an encrypted message can be "read" by a third party and the less likely a digital signature can be "forged". How strong the cryptography used in this country is is dependent on the state of Canadian cryptography policy.

On 1 October 1998, the Hon. John Manley, Minister of Industry, announced the results of an extensive review of Canada's cryptography policy. The balanced approach resulting from this review is designed to encourage the growth of electronic commerce; allow Canadian producers to export their products globally within the framework of international arrangements, and maintain the capability of law enforcement agencies to ensure public safety.

There are two main principles which underline the government's support of electronic commerce. First, Canadians are free to develop, import and use whatever cryptography products they desire. Second, no key recovery or licensing of certification authorities will be required. However, private sector issuers of keys will be encouraged to develop responsible practices such as key backup for data recovery purposes.[1] The Government of Canada, through its Public Key Infrastructure, will act as a model user of cryptographic products. As private sector certification authorities (C.A.'s) develop, the government will encourage the private sector to build accreditation mechanisms to ensure confidence and trust in their activities.

With respect to its obligations under the Wassenaar Arrangement (an international agreement governing the export of munitions and dual-purpose technologies), Canada will continue to leave in place cryptography export controls. However the application of these controls will consider the export practices of other countries and the availability of comparable products. In addition, the application process for export permits will be made more transparent and streamlined. The object is to minimize any regulatory intervention.

Insofar as the "bad guys" will use cryptographic products as well, the Criminal Code and other relevant statutes will be amended. The object of such amendments will be to criminalize the wrongful disclosure of keys and deter not only the use of encryption to conceal a crime but also the use of cryptography to conceal evidence. Existing interception, search and seizure and assistance procedures will be applied to cryptographic situations.

Protection of Personal Information and Electronic Documents Act

On 1 October 1998, Bill C-54 was introduced in the House of Commons. Divided into five parts, the bill is described in its summary:

> Part 1 of this enactment establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities, in connection with the operation of a federal work, undertaking or business or interprovincially or internationally.

[1] Keys can becomes lost or corrupted. Also, imagine a disgruntled employee encrypting all the data on his or her desktop and then destroying the private key, making all such information unrecoverable. There is a strong business case for employers to implement mandatory key backup policies.

> It establishes the following principles to govern the collection, use and disclosure of personal information: accountability, identifying the purposes for the collection of personal information, obtaining consent, limiting collection, limiting use, disclosure and retention, ensuring accuracy, providing adequate security, making information management policies readily available, providing individuals with access to information about themselves, and giving individuals a right to challenge an organization's compliance with these principles.
>
> It further provides for the Privacy Commissioner to receive complaints concerning contraventions of the principles, conduct investigations and attempt to resolve such complaints. Unresolved disputes relating to certain matters can be taken to the Federal Court for resolution.
>
> Part 2 sets out the legislative scheme by which requirements in federal statutes and regulations that contemplate the use of paper or do not expressly permit the use of electronic technology may be administered or complied with in the electronic environment. It grants authority to the appropriate authorities to make regulations about how those requirements may be satisfied using electronic means.
>
> Part 2 also describes the characteristics of secure electronic signatures and grants authority to make regulations prescribing technologies or processes for the purpose of the definition ``secure electronic signature".
>
> Part 3 amends the Canada Evidence Act to facilitate the admissibility of electronic documents, to establish evidentiary presumptions related to secure electronic signatures, and to provide for the recognition as evidence of notices, acts and other documents published electronically by the Queen's Printer.
>
> Part 4 amends the Statutory Instruments Act to authorize the publication of the Canada Gazette by electronic means.
>
> Part 5 amends the Statute Revision Act to authorize the publication and distribution of an electronic version of the Consolidated Statutes and Regulations of Canada.

The privacy provisions in Part 1 are based on the Canadian Standards Association's Model Code for the Protection of Personal Information. The Standard indicates how organizations who follow this Code are to collect, use and disclose personal information. It also addresses the rights of individuals to have access to their personal information and to have it corrected if necessary.

Part 2 is to be used to eliminate "paper-bias" in existing federal legislation. Part 3 is based almost entirely on the Uniform Electronic Evidence Act which was adopted by the Uniform Law Conference of Canada at its August 1998 annual meeting. One difference is a provision that permits the creation of evidentiary presumptions with respect to secure electronic signature technologies. The federal government's view is that in 1998 only one technology meets its criteria to be a secure electronic signature: digital signature technology.

Parts 4 and 5, in effect, will permit "official" on-line versions of the Canada Gazette as well as the consolidated statutes and regulations of Canada.

The Government of Canada Public Key Infrastructure

The Government of Canada is building a Public Key Infrastructure (GoC PKI)[2] to support the federal government's efforts with respect to electronic service delivery. In November of 1995, the Prime Minister decided on core responsibilities for the implementation and management of the GoC-PKI initiative. The Communications Security Establishment would be the location for the Canadian Central Facility (the "root") and a TBS-led interdepartmental group would oversee the implementation and policy management of the PKI initiative.

Currently seven Certification Authorities are cross-certified[3] on test platforms using three different types of X500 directories. It is anticipated that the GoC PKI will become operational in early 1999 as the CAs continue to upgrade their software and move to production platforms. External cross-certifications are expected to begin later in 1999.[4]

The establishment of a CA or community of CAs in a PKI can be described as "thirty per cent technology and seventy per cent policy". The basic "constitutional" documents for a CA are a Certificate Policy and a Certificate Practice Statement. The former indicates what a CA must do to manage the certificate(s) it issues. The latter specifies how the CA will meet those policy requirements. The Policy Management Authority of the GoC PKI has drafted a model Certificate Policy document.[5] Conforming to the PKIX Framework established by the Internet Engineering Task

[2] Current members of the GoC PKI include Treasury Board Secretariat, Communications Security Establishment, Royal Canadian Mounted Police, Department of Foreign Affairs and International Trade, Department of National Defence, Citizenship and Immigration Canada, Revenue Canada, Health Canada and Government Telecommunications and Informatics Services.

[3] The "connection" of one CA with another is done through the respective issuance of cross-certificates between the two CAs ("cross-certification").

[4] Technical interoperability trials were conducted during June 1998 with the National Computer Board of Singapore.

[5] This document provides four policies (rudimentary, basic, medium and high) for both digital signatures and confidentiality keys and may be found at http://www.cio-dpi.gc.ca.

Force, it is a technical document, which addresses the obligations of both the users of keys, and the CAs which issue them.

An Interdepartmental Task Force is developing a governance structure and policy framework for the GoC PKI. Treasury Board policy, inter-departmental memoranda of understanding, acceptable use policies, subscriber agreements and cross-certificate agreements are the tools which will implement the obligations outlined in the Certificate Policy document and meet other legal and policy requirements. It is anticipated that the policy framework will be in place in early 1999 before the GoC PKI Certification Authorities move onto their permanent platforms and formally begin to cross-certify. It is likely that federal departments will begin to implement PKI-enabled applications after completion of efforts to deal with Year 2000 issues.

It should be noted that federal/provincial/territorial Information Highways Ministers at their June 1998 meeting agreed to work together towards developing a common approach to implement a Public Key Infrastructure in Canada. At the international level, countries such as Canada, the United States and Australia see enormous potential for PKI-enabled applications to help serve citizens better.

Electronic Government

Government as an institution in society is not immune to the pressures and expectations to improve government through the application and use of technology. The Clerk of the Privy Council, in her Fifth Annual Report to the Prime Minister in April 1998, stressed the priority of electronic service delivery on the government's agenda and the need to ensure a secure electronic environment incorporating privacy and security protections.

Privacy and security concerns in an electronic environment were recognized in 1996 when the Treasury Board Secretariat (TBS) issued an Electronic Authorization and Authentication (EAA) Policy. This policy mandates the use of digital signatures to ensure the adequate control and protection of "internal" government transactions in electronic form. Existing electronic business systems were obliged to comply with this EAA policy as of July, 1998.

The federal government is responding to its clients - the public – by renewing how it operates, manages and provides programs and services. Some examples include:

Government Telecommunications and Informatics Services (GTIS) is developing a *Secure Applications and Key Management Service (SAKMS)* to provide federal departments with a portfolio of Certification Authority services: key management, certification service, client support, Local Registration Authority, and training. Additional services, such as Secure Remote Access and other customized services, are also available. These services are operational, functioning and being used by a number of departments and agencies.

Industry Canada has a pilot project for the electronic filing of information under the Investment Canada Act. This involves processing approximately 1,000 applications each year from 200 legal firms across Canada.

Industry Canada is also developing a *Spectrum Radio Licensing Pilot* involving the submission of radio spectrum licensing applications: up to 750,000 applications annually involving fees of over $150 million. This pilot provides a secure means to file applications and also includes access to established databases

The National Energy Board intends to create a secure electronic regulatory process for approximately 750 applications per year. The pilot uses PKI technology for the electronic filing of applications and involves electronic document management and an on-line information repository.

Conclusion

The Internet is changing how we communicate and transact business. A logical extension of this type of activity is the delivery of government services using technological means. Governments – at all levels - in Canada are beginning to re-engineer business processes to do just that – both to increase their own efficiency and to serve as model users for the private sector.

In providing "electronic government", there is a sensitivity on the part of government to protect individual privacy and ensure the confidentiality of personal information travelling over public networks. At the federal level, this has resulted in the development of an infrastructure using public key cryptography to provide that privacy and security. We are starting to see pilot projects to demonstrate "PKI-enabled" means of dealing with the federal government.

With respect to policy development at the federal level, the government has developed an e-commerce strategy. Part of that strategy involves a revised cryptography policy and legislation that addresses privacy concerns and enables statutes to be made "media-neutral". For its own activities, the federal government has put in place an electronic authentication and authorization policy for GoC personnel. "Electronic government" or government using electronic means to "do" things is becoming more of a reality in 1998.