Legal Framework for E-Government

The Canadian Experience

Presentation to RED GEALC Workshop
Rhonda Lazarus
Lazarus.Rhonda@tbs-sct.gc.ca
March 6, 2006
OUTLINE OF PRESENTATION

• Canada’s Starting Point
  • Context
    • definition of E-Government
    • Federal, Provincial & Territorial Governments

• Frameworks to Enable E-Government
  • International harmonization: UNCITRAL; Commonwealth; ULCC & PIPEDA
  • Lessons Learned

• Using the Framework
  • Implementation at the Operational Level – What else is needed?
  • Privacy, Security, Technology

• The Way Forward
  • New Challenges; Successes
  • Law Reform
Governments and laws in Canada

CONTEXT:

DEFINITION OF E-GOVERNMENT

“the use of ICT to promote more efficient and effective government, facilitate more accessible government services, allow greater public access to information, and make government more accountable to citizens. E-government might involve delivering services via the Internet, telephone, community centers (self-service or facilitated by others), wireless devices or other communications systems.”

http://www.redgealc.net/

Federal, Provincial and Territorial Governments = 14 governments!

STARTING POINT:

Identifying impediments to electronic communications in existing legal framework
Statute; common law have paper bias: “writing”, “signature”, “copy”, “original”
Court decisions seemed to accommodate e-commerce
Risk assessment – how risk-tolerant can we be?

IS E-GOVT. LEGAL?

Eliminating uncertainty is necessary to foster a climate conducive to use of electronic media in Government and in business
FRAMEWORKS FOR E-GOVERNMENT

• Co-ordination and collaboration needed to address legal impediments, both domestic and international

• Avoid creating new impediments or exacerbating trade obstacles by failing to harmonize new legislative schemes

• INTERNATIONAL LEVEL –
  – UNCITRAL MODEL LAWS
    • Electronic Commerce, 1996
    • Electronic Signatures, 2001
    • Convention for Electronic Contracts 2005
  – Commonwealth Model Bills
    • Electronic Transactions
    • Electronic Evidence 2000 Endorsed for use by Commonwealth countries by Law Ministers November 2002
CANADA’S APPROACH

- UNIFORM LAW CONFERENCE OF CANADA
  - Uniform Electronic Commerce Act
  - Uniform Electronic Evidence Act
  - Most provincial and territorial governments have enacted legislation modelled on uniform laws

- UECA comprehensive minimal, flexible scheme –
  - Allows governments to deliver programs and services electronically
  - Allows citizens and businesses to provide information to government electronically by reliable means
  - Permits parties to enter into contracts
  - Technology neutral – does not favour one technology over another
  - Allows government to specify what an electronic document has to have or be so that it is equivalent – as reliable – as paper
  - Principle of consent – technology not imposed on government, businesses or citizens
CANADA’S APPROACH cont’d.

• **Uniform Electronic Commerce Act**
  - Electronic document can satisfy a statute’s:
    - Writing requirement
    - Signature requirement
    - Requirement for an original or copy
  
  - Authorizes Governments to specify what methods businesses and citizens will use in sending information to Government and, in certain circumstances, between themselves

  - Confirms contracts can be made by electronic means, e.g. clicking a mouse, touching a screen, speaking to computer
    - Sequence of offer and acceptance is clarified, and can be automated
CANADA’S APPROACH cont’d.

• **Uniform Electronic Evidence Act**
  - Sets out functional equivalent of “best evidence” rule
    • Before— best evidence rule needed original document, because indicated integrity and trustworthiness of content
    • But what is an “original” or “copy” in electronic environment?
    • After— prove reliability and integrity of electronic document through evidence of reliability of record-keeping system
    • Presumption of integrity is raised through affidavit and subject to cross-examination
  
  = Encourages good record-keeping practices
PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT, 2001

• PIPEDA
  – Part 1 deals with privacy in federally-regulated private sector
  – Part II – Electronic Documents part
  – Part II applies to federal statutes and regulations
    • Statutory requirements for paper can be met by electronic documents if:
      – Statute is listed in a schedule (by order), to provide notice to the public that the program or service is available electronically; and
      – Regulations enacted to stipulate what technologies Government will accept, among other things.
    • In some cases, document must be signed with a SECURE ELECTRONIC SIGNATURE; e.g. affidavit; certificate; original
SECURE ELECTRONIC SIGNATURES

• **Secure Electronic Signature** (s. 48) must be:
  
  • Unique to the person;
  • Under the sole control of the person
  • Used to identify the person
  • Linked to the document and can determine if document has been altered

  – Regulations specify digital signature technology (Public Key Infrastructure) supported by digital signature certificates = **Secure Electronic Signature**

• **Canada Evidence Act**, ss. 31.1 to 31.8: When SES is used in an electronic document, it is presumed to have been signed by the person identified in the signature certificate
LESSONS LEARNED

• PIPEDA -
  – Opt-in process onerous
  – Need to train program managers and legislative drafters
  – Important that policy, legal and technology experts work together
  – Instrument choice – regulations not as flexible or speedy as we had anticipated

• Important to have harmonized legislation; look at existing model laws, including Commonwealth model legislation

• Laws should be media and technology neutral

• Consent-based – do not impose technology on individuals – not all have access to it
USING THE FRAMEWORK for E-GOVERNMENT

• GOAL:
  – To encourage Canadians to embrace Internet as their choice of channel to communicate with GoC

• WHAT ELSE DO WE NEED AND HOW DO WE GET IT?
  – Laws alone are not enough
HORIZONTAL SERVICES; GOVERNMENT ON-LINE and SHARED ADMINISTRATIVE SERVICES

• Horizontal Services
  – What do Canadians want? We asked, and they answered:
    • Privacy and Security – concern about sending private information over the Internet
    • Multi-channel access to government services and information – people want to be able to choose to access Government by telephone, ordinary mail, in person and by Internet
    • One-stop shopping; No wrong door – integrating/joining up similar services to make them easy to find and easy to deal with
    • Within Government, sharing administrative services like payroll, procurement, may be efficient and cost-effective

• CHALLENGES
  – Government is structured in stovepipes; over 150 departments
  – Privacy Act and enabling laws for departments create barriers
  – Ministerial accountability to Parliament can result in lack of coordinated approach across Government
BREAKING DOWN THE SILOS

• **GOL** – collaborative services mean taking down departmental barriers to provide seamless, transparent and convenient access to Government information and services
  – At the same time, we need to ensure that we protect the privacy rights of our citizens and that we secure their information from attack

• **Shared Administrative Services** – also need to take down departmental barriers within the Government, while protecting the privacy rights of our employees and securing their information from attack

• **OPTIONS**
  – Continue with work-arounds, but not transparent and not scaleable
  – Amend *Privacy Act*
  – New legislation for horizontal and integrated programs a possibility
MORE LESSONS LEARNED
-the lawyer’s perspective

- HOW TO DESIGN AND IMPLEMENT A PROJECT
  - Critical factors are interdependent; change one, change all
    - Privacy, security, legal implications evolve as program design progresses- want to avoid “show-stoppers” early on
    - Teamwork is critical – please involve the lawyers early in the program design!
      - ongoing legal risk assessments of departmental authority, compliance with laws, like Privacy Act, Charter of Rights and Freedoms, program-specific statutes
      - lawyers need to understand what the technology does, and technology experts and program managers need to understand what the law requires, so they have to learn to speak each others’ language
  - Legal analysis requires detailed and understandable description of data-flow
MORE LESSONS LEARNED
-the lawyer’s perspective .. 2

• Legal Education and Guidance
  – Each department has its own lawyers; varying levels of specialization in information technology law
  – Department of Justice E-commerce Committee used as tool for bringing clients together with lawyers
    • Helped to bring new issues to attention of Justice legal community, and vice versa
    • Created useful network for open discussion of issues and means to resolve them, so helpful to client departments and lawyers, especially because Government issues differ from private sector
    • E.g. Call letter to all legal services to determine the legal issues that were creating barriers to program implementation, with objective of finding government-wide solutions, whether legislative, policy, or technological
IN BRIEF, SUCCESS FACTORS:

• TO BE SUCCESSFUL:
  – Solutions need to integrate Law, Technology, and Policy
  – Need Government-wide collaboration and coordination of lawyers, policy-makers, program managers, and techies
  – Need IT Security and Protection of Privacy
  – Need means to authenticate where necessary or appropriate, with anonymity being the default setting (based on threat/risk assessment)
  – Need a Government Champion, with financial resources in support, and accountability to Parliament
  – Need interoperability and integration of services
OTHER CYBERLAW REFORMS

• **Criminal Code of Canada**
  - Enabling and using technology leads to other challenges
  - Should not facilitate E-Government without strengthening criminal laws
  - Our *Criminal Code* while not drafted for cybercrime, is able to cover many offences –
    - *Section 327* – possession of device to obtain telecommunications services
    - *Section 342.1* – unauthorized use of computer
    - *Section 430* – mischief
  - Recent amendments to *Criminal Code* made to allow systems owners and managers to intercept a private communication without a warrant in order to defend their computer networks and databases from attack (Intrusion Detection)
OTHER CYBERLAW REFORMS contd.

• New threats will continue to appear and need constant vigilance
  – **Identity Theft:**
    • Used to commit fraud, acts of terrorism, theft of services
    • Canada and U.S. work bilaterally to combat through coordination and awareness
    • U.S. has specific legislation; Canada can rely on existing forgery, fraud, personation offences
  
  – **SPAM:**
    • Wastes resources, space, can crash systems
    • Spam Task Force report recommended statutory clarification
    • Need for international cooperation for cybercrime
USEFUL REFERENCES

• Uniform Law Conference of Canada
  – http://www.ulcc.ca/

• Uniform Electronic Commerce Act and Commentary

• Uniform Electronic Evidence Act and Commentary

• Report of the Spam Task Force

• PIPEDA

• SES Regulations

• Government of Canada’s Legal and Policy Framework for GOL,
  http://www.solutions.gc.ca/pki-icp/gocpki/frame/frame00_e.asp