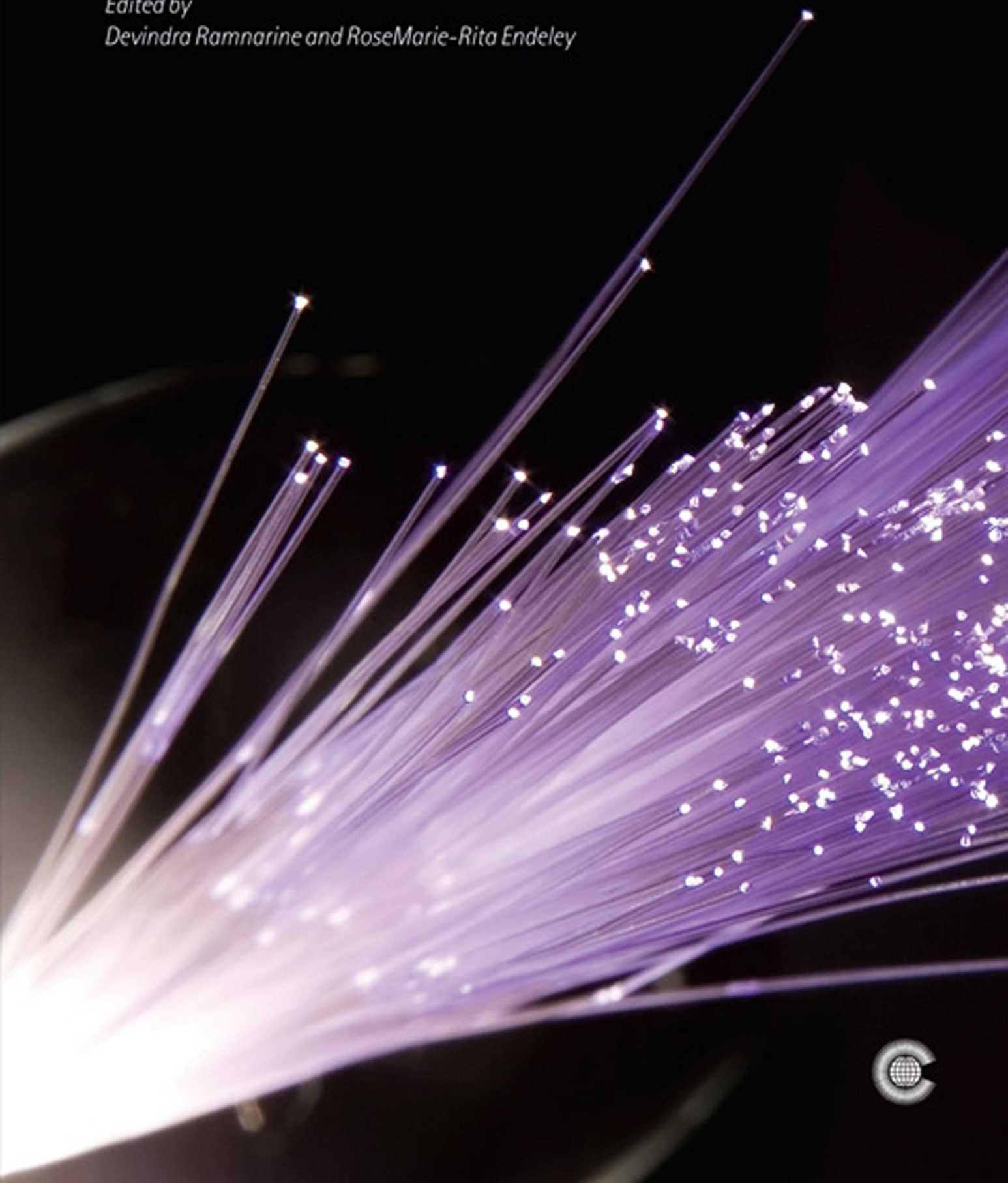
Information and Communication Technologies for the Public Service

A Small States Focus

Edited by
Devindra Ramnarine and RoseMarie-Rita Endeley



Information and Communication Technologies for the Public Service

A Small States Focus

Information and Communication Technologies for the Public Service

A Small States Focus

Edited by
Devindra Ramnarine and RoseMarie-Rita Endeley

Commonwealth Secretariat

Published by
Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom

© Commonwealth Secretariat 2008

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or otherwise without the permission of the publisher.

Published by the Commonwealth Secretariat
Edited by Jane Lanigan, Editors4Change Ltd
Designed by S.J.I. Services, New Delhi
Cover design by Tattersall, Hammarling and Silk

Printed by RPM Print and Design

Views and opinions expressed in this publication are the responsibility of the authors and should in no way be attributed to the institutions to which they are affiliated or to the Commonwealth Secretariat.

Wherever possible, the Commonwealth Secretariat uses paper sourced from sustainable forests or from sources that minimise a destructive impact on the environment.

Copies of this publication may be obtained from
The Publications Section
Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom
Tel: +44 (0)20 7747 6534
Fax: +44 (0)20 7839 9081
Email: publications@commonwealth.int
Web: www.thecommonwealth.org

A catalogue record for this publication is available from the British Library.

ISBN: 978-0-85092-878-5 (paperback)
ISBN: 978-1-84859-008-3 (downloadable e-book)

Contents

Foreword

The public sector in many Commonwealth countries has undertaken a variety of e-governance and e-government projects to exploit the use of information and communication technology (ICT). While there are significant benefits associated with these large and complex change initiatives, there are also many challenges that will be encountered during the journey towards e-governance and e-government.

This publication, *Information and Communication Technologies for the Public Service: A Small States Focus*, provides the lessons and experiences from a number of Commonwealth small states that have pioneered the electronic delivery of public services. The publication outlines the major concerns associated with e-governance for effective service delivery, including a synopsis of issues, experiences and international efforts in these countries. It also recommends steps that can be taken to move the deployment of e-governance forward.

I wish to thank Professor Thomas B Riley, Executive Director, and Mr William Sheridan, Research Fellow, Commonwealth Centre for e-Governance, Ottawa, Canada, for their detailed research work and the bulk of writing involved, especially the time taken to analyse and structure the contents of the numerous materials produced at the workshops. I acknowledge the tireless efforts of the editors: Mr Devindra Ramnarine, Adviser, Public Sector Informatics, Governance and Institutional Development Division (GIDD) and Head of Commonwealth CONNECTS; and Dr RoseMarie-Rita Endeley, Adviser, Caribbean and Mediterranean Region, GIDD, for conceptualizing and executing the successful activities and interactions that have contributed to the knowledge and best practices contained in the publication.

Dr Albert Tan of Singapore and Mr John Wilkins of the Commonwealth Secretariat presented several case materials at the workshop. The following officials also addressed the workshop and were integral to its success: Mr Peter Gough, Deputy Head of the Civil Service; the Hon D Kurt Tibbetts, JP, Leader of Government Business, Cayman; Dr Hassan Syes, President, University College Cayman Islands (UCCI); Mr David Spiteri Gingell, Chairman, Malta Information Technology and Training Services Ltd (MITTS); and Mr Devindra Ramnarine and Dr RoseMarie-Rita Endeley, both of the Commonwealth Secretariat.

Finally, the Commonwealth Secretariat appreciates the valuable contributions from all delegates and representatives who participated in the various workshops in the Caribbean and Mediterranean countries.

Mrs Jacqueline Wilson
Director, Governance and Institutional Development Division
Commonwealth Secretariat
London SW1Y 5HX
United Kingdom

Acronyms

APQC	America Productivity and Quality Centre
BPR	Business process re-engineering
CIDA	Canadian International Development Agency
CARICAD	Caribbean Centre of Development Administration
CIMU	Central Information Management Unit (Malta)
CRM	Customer relationship management
DES	Data Encryption Standard
EC	European Commission
ERD	Department of Employment Relations (Cayman Islands)
ESRI	Environmental Research Systems Institute
GIS	Geographic information systems
GIDD	Governance and Institutional Development Division (of the Commonwealth Secretariat)
G-B	Government-business relations
G-C	Government-citizen relations
ICTs	Information and communication technologies
OHS	Occupational Health and Safety
OWS	Office and Workplace Services
OECD	Organisation of Economic Co-operation and Development
PKI	Public Key Information
PPP	Public-private partnership
TASF	Technical and Advisory Support Facility
UNDESA	United Nations Department of Economic and Social Affairs
UCCI	University College Cayman Islands
VPN	Virtual private network

Introduction

Electronic infrastructure and network functionality are being utilised by governments around the world. The history of how and why ICTs (information and communications technologies) came into government use is an important part of the story of their success to date and their prospects for the future. There have been three parallel trends that account for the current circumstances with regard to the decisions by developing countries to adopt e-government. The first trend involves the origins of widespread network processing, which began with business applications and received the name **e-commerce** from its users. The success of these ventures (credit card processing, online catalogues and sales etc.) impressed those in government, and inspired the public to ask their governments to move in the same direction.

The second trend concerns the sequence of locations where e-government operations were implemented. As would be expected, those countries initially possessing the most electronic and network infrastructure for public and business use were also the first to adopt these technologies for government use. The success of e-government in developed countries served as **demonstration projects** for the less developed countries. They began to buy equipment and build their own systems, often with assistance from countries and organisations that already had e-government and could share their experiences and lessons learned.

The third trend entails the broadening of the concept of using electronic infrastructure and network functionality for government operations. All countries started out with the term **electronic government** to describe their use of email and the Internet for both internal and external communications. However, expectations subsequently increased to include the possibility of electronic consultation (with the public), electronic transactions (paying taxes and user fees) and electronic voting. As a result of the inclusion of all of these forms of interaction, the general process involved in mediating them is now referred to as **electronic governance**.

This book begins with three chapters, one for each of the trends identified above, so that the social, political and technological context of e-government and e-governance in developing countries can be clearly understood. The fourth chapter is devoted to some of the considerations involved for implementing e-governance and e-government. These contextual chapters are followed by chapters that report on the contents and conclusions of a workshop on the use of ICTs for improving public service delivery that was developed by the Governance and Institutional Development Division (GIDD) of the Commonwealth Secretariat and supported by the Government of the

Cayman Islands, with participation by the countries of the Caribbean and the Mediterranean. This workshop was held in Grand Cayman between 4 and 8 June 2007. The concluding chapter considers some of the issues relating to privacy and information technology security that arise in pursuing an e-government/e-governance agenda.

Dr Albert Tan of Singapore, Mr Devindra Ramnarine of the Commonwealth Secretariat and Mr David Spiteri Gingell of Malta presented the main case materials at the workshop. The following officials also addressed the workshop: Dr RoseMarie-Rita Endeley of the Commonwealth Secretariat; Mr Peter Gough, Deputy Head of the Civil Service, Government of the Cayman Islands; the Hon. D Kurt Tibbetts, JP, Leader of Government Business, Cayman Islands; Mr John Wilkins of the Commonwealth Secretariat; and Dr Hassan Syes, President, University College Cayman Islands (UCCI). The countries with representatives participating in the workshop and whose inputs are incorporated into this book, include: Anguilla, Bahamas, Barbados, Belize, Cayman Islands, Cyprus, Grenada, Guyana, Jamaica, Kenya, Malawi, Mauritius, St. Kitts and Nevis and Trinidad and Tobago.

Chapter 1 traces the progression of the application of electronic operations **From e-Commerce to e-Government**. This trend is particularly relevant because the materials presented in the workshop by Dr Tan rely heavily on the World Bank perspective on electronic government, which in turn is premised on the importance of the transfer of electronic commerce methods to design and implement electronic government.

Chapter 2: **From Developed to Developing Countries**, outlines how electronic government was initially designed and deployed in developed countries, whereupon, through the demonstration effect, developing countries could see the results and chose to adopt similar methods for their own governments. It is appropriate to review this trend because the Organisation for Economic Co-operation and Development (OECD), the Commonwealth Secretariat and a number of other international organisations that have guidelines on the acquisition and operation of electronic government, base much of their advice on the experiences gained and lessons learned from developed countries.

Chapter 3 explores the transition **From e-Government to e-Governance**, from the initial strategy of information dissemination to the later advancements towards electronic transactions (between and within governments, between governments and citizens, and between governments and businesses) and e-democracy (electronic voting and electronic participation in consultation with governments).

Chapter 4, on **Implementing e-Governance and e-Government**, reviews the conditions that are involved in assessing readiness for e-governance and e-government, and the challenges encountered when implementing citizen-centric government in response to the desires the public has consistently expressed in a variety of surveys.

The content of chapters 5, 6, 7 and 8 is largely based on materials from the Commonwealth Secretariat workshop (entitled the 'Regional Workshop on e-Government Readiness for Effective Public Service Delivery'), which took place 4–8 June 2007 in the

Cayman Islands. Chapter 5 presents an overview of the current state of **Electronic Government in Barbados and the Cayman Islands**. Some examples are used to illustrate notable instances of success with government service delivery, or to show the plans that have been developed to adopt e-government in the foreseeable future. Chapter 6 provides a summary of the themes and conclusions of the materials presented at the workshop itself, while chapter 7 develops a comparative analysis of the plans of, and prospects for, **Electronic Government** in the countries participating in the workshop. Finally, chapter 8 presents an international survey on **Privacy and Information Technology Security.**

1

From e-Commerce to e-Governance

The technology platform

Electronic governance (e-governance) is a spin-off from electronic commerce (e-commerce). In many respects, the modalities and functions that were developed initially in e-commerce have subsequently been transferred to governments, albeit in forms suitable to public administration rather than corporate administration.

In both e-commerce and e-governance, the 'electronic' component is provided by a combination and integration of computers and communications networks. The basis for the computer contribution has been the growing capabilities of hardware and software. In the case of the communications networks, new technologies and improved communications protocols had to be added to hardware and software to enable email and create the World Wide Web.

What this electronic platform provides is the capability to provide more effective and efficient governance using computers and communications. In e-commerce, the first use of the Internet was to distribute advertising and documentation more quickly, more widely and more cheaply. The initial exercises in e-governance were essentially the same. Government departments posted publicly available documents on '**the web**' to reduce printing and mailing costs.

Electronic functionality

Commercially, email was first used for internal co-ordination of operations and customer feedback. Government departments adopted similar uses. Colleagues used email to facilitate workflow and co-ordinate projects. E-mail links were also listed on Internet documents so that the public could follow-up with questions or suggestions about the government materials they were accessing and downloading.

The next phase of e-commerce involved selling over the Internet by taking orders for products via electronic forms. Payments for these transactions were enabled by the development of secure credit card processing arrangements. Tangible goods could be shipped to the purchaser by mail or courier, and intangible goods (software, electronic books and reports etc.) could be transmitted back as soon as the transaction was confirmed. Governments followed suit by collecting data with electronic forms (census etc.), accepting payments of fines and fees with card transactions, and selling publications and data in the same manner as is done with e-commerce.

Most businesses now have websites, as do most government departments. The latest developments have been to engage customers or citizens in consultations, either in some form of marketing research for companies, or policy research for governments. And just as increasing numbers of customers can make purchases electronically, so governments are also enabling electronic voting for citizens. In both businesses and governments, more and more of the co-ordination and communications throughout their organisations is being conducted electronically, and then stored and retrieved in that format as well. At the same time, since the technology is continually evolving, the need for updating and expansion requires ongoing investment and successive plans for change management.

Responding to deficiencies

A number of early evaluations of e-commerce and e-governance have concluded that these projects were only limited successes or outright failures. The shortcomings most frequently cited were missed deadlines, cost over-runs, unworkable technologies and training inadequacies. Compounding these difficulties was the situation with less developed countries, where the desire to achieve the benefits of e-commerce and e-governance was complicated by the lack of resources and trained personnel with which to build the infrastructure, and the lack of widespread connectivity of the wider public whereby to access such electronic services.

In response to such problems regarding e-governance, several governments, consultants, public interest groups and inter-governmental organisations researched the deficiencies and developed guidelines to alleviate them, both for more developed and less developed countries.

What next for e-governance?

The next challenges for e-governance within the Commonwealth will be similar to those faced wherever electronic networks prevail. Perhaps the most important characteristic of future developments is that they will diverge significantly from the e-commerce patterns of the past.

There seems to be a growing expectation amongst members of the politically-interested public that the culmination of trends in e-governance will result in full-fledged participatory democracy. People will want to be consulted and involved in policy development and regulatory specification in whichever areas they are concerned about. This is the long-term implication of ubiquitous networks and the concept of 'Citizens As Partners'. Both elected and appointed officials will still have the lead role in governance; **however**, the public will want evidence that their views are solicited, respected and factored into the governance process.

Another major role of e-governance will continue to be service delivery. There are contradictory requirements in this area. In so far as service provision depends upon individual eligibility (payment of taxes, fees, fines etc., and authorisation and/or

distribution of particular benefits), access can be customised by being based on specific personal profiles for every user. However, the public will only find this acceptable if files and databanks are not cross-referenced or used for enforcement of policies extraneous to the purpose for which the data is collected. The balance between customisation and confidentiality will have to be carefully crafted and continuously revised to reflect the changing nuances of public opinion.

Ongoing challenges for Commonwealth e-governance

The hidden side of e-governance will continue to involve the co-ordination of governmental internal operations. In many cases there are various idiosyncratic versions of the same functional processes, with the only justification for this diversity being the historical variability of different departments and agencies. The workflow is often too segmented, resulting in too many procedures, authorisations and personnel required for what could be simplified, faster, less costly activities. Those responsible for internal e-governance will continue to be pressed to squeeze additional efficiencies and expenditures out of these processes, in part so that the funds saved can be re-allocated to support the expanded public side of e-governance.

The most controversial e-governance issue of all, at least to date, is the trade-off between national security needs and open government expectations. Not surprisingly, national security practitioners base information sharing on the 'need to know' concept. Equally obviously, advocates of open government talk about 'the public's right to know'. If these two choices are placed along one dimension, the other orthogonal dimension for this issue would dichotomise political acceptability vs. constitutional constraints. Together these two dimensions would create a matrix with four types of policy options. Some sectors of the public will always want more information, and some sectors of the security establishment will always be able to rationalise why they think less information should be provided. Every choice requires political judgment – as such there are no hard and fast rules.

Conclusion

Because e-commerce set the precedent by developing before e-governance, and because each does incur direct and indirect costs, the question of who pays for both accessibility and services very quickly becomes an issue. Even though electronically-provided services save considerable money compared to printed matter and personal services,

Table 1.1 Trade-off between national security and open government

E-governance trade-offs between national security vs. open government		**Basis of information sharing**	
		The need to know	*The right to know*
Policy rationales	*Political acceptability*		
	Constitutional constraints		

the costs of extending networks and local accessibility, and of posting and updating web materials, may over the long run actually exceed the previous expense of more conventional service delivery.

It is the existence of this cost-barrier that is the major cause of the digital divide. The correlation of lower incomes with certain other social characteristics such as locality, ethnicity, education, occupation and gender, puts many of groups at a disadvantage regarding access to either e-commerce or e-governance.

The issue of the 'digital divide' will continue to draw attention, both in developing countries and amongst lower-income groups in developed countries. In fact, the Commonwealth Heads of Government at their 2005 and 2007 meetings in Malta and Uganda respectively encouraged and endorsed the Commonwealth Secretariat's Commonwealth Connects Programme as their flagship initiative to address the pressing digital divide challenge in the Commonwealth (see www.commonwealthconnects.net for further details). The initial definition of the digital divide focused on the presence or absence of connectivity. The combination of community-based facilities and improved incomes is slowly addressing this version of the digital divide, but there are still many people without either computers or telephones. A lot more infrastructure is required, and governments may have to be the major providers because the private sector may not see either a quick enough or large enough pay-back to make the investment worth their while.

The other aspect of the digital divide is the relevance of the information that is available even if connectivity is established. Different groups (depending on age, gender, income, education, occupation and service needs) want different types of information from their governments: 'One size does not fit all'. As a result of this growing recognition, website materials are being formatted and categorised to suit different clienteles. This trend will likely accelerate, and the only effective basis for it seems to be ongoing surveys of public information needs. Updates, revisions and new materials will have to be provided in a more timely fashion, to reflect the accelerated pace of change that the Internet is contributing to.

What the history of e-governance reveals, however, is that in the Commonwealth, as elsewhere, it is here to stay. The public now expects it, and furthermore expects its performance to improve in the foreseeable future. That is the goal towards which all Commonwealth governments should aim.

2

From Developed to Developing Countries

Introduction – framing the issues

As will be shown in this chapter, much of the literature in the academic world reflects the important dichotomies between the developed countries' approach towards e-government and the obstacles facing developing countries. In summary, the challenge that developing Commonwealth countries face is that many of them still do not have either the advanced industries or the financial wherewithal to duplicate in all respects what their fellow members have achieved in the more developed countries. At the same time, however, public expectations are building to the same extent as they did elsewhere regarding the desire to modernise governments and their service delivery. Such a discrepancy, which sets the growing desire for change against the financial constraints on implementation, faces the Commonwealth system with a unique dilemma.

Fortunately, the tradition of co-operative endeavour is enabling the Commonwealth to tackle this situation successfully. By way of three approaches, e-government is reaching all corners of the Commonwealth, in that developing countries are: (1) identifying their ICT needs for e-government; (2) avoiding the pitfalls by tracking the lessons learned in other countries; and (3) focusing infrastructure acquisition and deployment on their particular service needs.

The way that developing Commonwealth countries are identifying their ICT needs for e-government is through '**benchmarking**'. A benchmark is a structural comparison or performance test of hardware and/or software[1] . A number of international organisations have conducted benchmarking studies of both developed and developing countries' efforts to apply ICTs to workflow, horizontal integration, service delivery and public consultation. By observing what others have accomplished, it is possible to pick and choose the best in the particular circumstances of each government.

The most effective technique for avoiding the pitfalls of previous projects is by tracking the lessons learned in other countries through seeking and applying **best practices**. The term refers to 'effective ways to perform processes or sub-processes that have been identified inside or outside' the organisation[2] . Lists of best practices have been published for the benefit of new projects in business and government. Infrastructure acquisition and deployment between different organisations or projects is called

'**technology transfer**'[3]. For some aspects of e-government, turnkey packages are available that will provide total systems for specialised functionality. In other cases, consultants can analyse and design a customised solution that includes such transfer elements as new equipment, software upgrades and ongoing user training.

Benchmarking

The procedure of benchmarking is now considered one of the standard methods in a manager's 'tool kit'[4]. In her description, Dr Suzanne Turner, University of Warwick, advises use of the technique whenever 'you are interested in learning from other organisations ways to improve your own organisation'[5]. There are a number of different ways to use the procedure, including either in-house observation or external comparison, and either staff conducted or professionally contracted benchmarking. In the case of benchmarking between countries, external comparisons and professional contracts would usually be the means deployed.

The European Commission, of which the United Kingdom is a member, sponsored a conference in Manchester, UK, in 2005 to compare governments' readiness for e-government projects[6]. Concurrently, research from a New Zealand academic focused on the impact that national cultures were having on worldwide readiness for e-government[7]. The School of Computing at Middlesex University is now offering PhDs to international students that consist, in part, of a study of e-government readiness in their respective countries. One notable example compares Egypt, the United Kingdom and Dubai[8]. The Victoria University of Wellington, New Zealand, has recently appointed the first Professor of e-government in the world.

Governments themselves sponsor some of the benchmarking studies. The e-Government Resource Centre[9] is a dynamic site hosted by the Government of Victoria, Australia, and aims to help everyone learn from each other and continue to be the pacesetters in using new technologies to deliver better government services. International financial institutions are also advocates of electronic government, with the view to increasing transparency and reducing corruption. The World Bank has a website devoted to teaching and assisting users with e-government[10]. One particular paper on this website covers sectors, stages, opportunities and challenges of online government.

What this sampling indicates is that there is an abundance of materials available that 'benchmark' (compare) the efforts of numerous national and regional governments to install and operate e-government. All of this material is available to Commonwealth countries, as are the invitations of many of the sources of material for countries to seek further information and/or help in studying and analysing their own situations, and in designing and deploying their own solutions.

Any government of a developing Commonwealth country that is seeking helpful comparisons of these kinds of projects may find the following guidelines useful:

- create a team of stakeholders to design a benchmarking survey;
- ask the stakeholders' team to craft a list of functionality requirements; and

- understand the local context and environment of the benchmarked projects.
- look for comparisons of hardware, software, and 'peopleware' (human issues);
- seek comparisons of both similar and dissimilar situations to your own;
- search for comparisons of costs, duration and disruption of e-government projects;
- find out how much was devoted to training (half the project cost is appropriate);
- enquire about sources of financing that different projects have used; and
- ask technology suppliers to compare projects they have implemented.

Best practices

The American Productivity and Quality Centre (APQC) is an internationally respected think tank advocating the use of ICTs to increase productivity and improve quality. Tracking and trading best practices is one of its major endeavours, which it defines as 'an assessment recommending the most appropriate way of handling a certain type of task, based on an observation of the way that several organisations handle that task'[11].

Business consulting has the most experience with best practices to date, because commercial firms were the first to get into digital transactions and networked organisations. Best practices have now accumulated to the extent that large consulting companies often assign specialised groups exclusively to leveraging best practices knowledge[12]. Businesses that use best practices, and the consultants who can advise on them, are already practicing in Commonwealth countries, both developed and developing. Developing countries can use private sector expertise to move forward with e-government by partnering arrangements that could share experience and lower costs.

The European Commission maintains a website devoted to the e-government best practices of its members[13]. There is a Good Practice Framework on this website, the main objectives of which can be useful to all Commonwealth countries:

- to collect examples of well-defined e-government cases;
- to create an intelligent knowledge database of those involved in e-government;
- to provide easy access to e-government know-how and expertise; and
- to support the sustainable transfer of good practices.

Academic organisations have also taken a deep interest in e-government for developing countries. The 'e-Government for Development Information Exchange' Project is co-ordinated by the University of Manchester's Institute for Development Policy and Management[14]. This website covers five e-government topics, namely:

- Topic 1. Building e-government websites;
- Topic 2. m-government – mobile/wireless applications in government;
- Topic 3. Public sector health information systems;

- Topic 4. Using ICTs for government transparency; and
- Topic 5. Achieving success/avoiding failure of e-government projects.

The last topic of this list will be one of the most useful for less developed Commonwealth country governments seeking to digitise. Questions about actual or possible project failures are posed and then answered in such a way as to alert those contemplating further e-government, so they can recognise many pitfalls:[15]

- Why do failures occur?
- How costly are failures?
- What can be done to avoid failures?
- Where to get training on e-government successes and failures? [Online manual.]

Technology transfer

Building effective e-government facilities follows a supply-chain process: research, analysis, design, planning, deployment, training, operations, feedback and improvement. Although any of these steps might conceivably be either expanded into sub-routines, or contracted into larger steps, these activities are both recognisable and manageable. Further, depending on the resources available, not all these steps need to occur in a single linear process – some may run in parallel, depending upon the size, scope and strategy of the project. However, all these steps have to be properly engaged if the project is to succeed. In this respect, e-government projects resemble many other public policy initiatives, which will come as no surprise to Commonwealth governments.

Governments in Commonwealth countries, and in most other countries for that matter, want the acquisition and operation of e-government systems to be accompanied by technology transfer. They want not only to be the owners of the infrastructure, but also to be the masters of its design, operation and future development. The exercise of both national sovereignty and political stability depend upon these capabilities. There are different visions about how to accomplish these goals, though they will lead to different versions of technology transfer.

One approach to e-government seeks to focus primarily on digitising service delivery to the public[16] . Documents could be delivered to the public electronically, saving money and speeding dissemination. Developed Commonwealth countries began with this approach, and are now moving beyond it. With this approach, there has also been some talk of government operations with fewer employees per service process, a prospect that has more recently been downplayed in favour of 'improved service delivery'.

Of course, there is a caveat to this suggestion. In most developing countries, there is limited access to electricity, water and other life essentials. Poverty and literacy need to be addressed first, with technologies being enhancers of the process of change. Assessments of needs are the first step in helping a developing country to make effective use of ICTs.

A second approach revolves around improving the policy-making process through electronic workflow and horizontal co-ordination[17]. Silos of information and stovepipes of policy-making are slowly being reproached and replaced as the public demands. The rationale offered for this approach is that more co-ordination will reveal existing contradictions in statutes and regulations, and avoid them in new ones. The outcome will be policy integration, on the assumption that the public wants understandable programmes rather than jurisdictional roadblocks. Developed Commonwealth countries are now in the midst of implementing this approach, encountering more inconsistencies and resistance than was initially expected.

A third approach, just recently started, is to increase public consultation and participation in policy-making. One aspect of this approach is to invite the public into the policy process via electronic networks that deal with specific issues and operate under controlled formats[18]. The other aspect of this approach is to take network accessibility to the public, often in the form of community informatics, to act as a combination of economic-social-political infrastructure, so that poverty does not continue to perpetuate the digital divide[19].

Commonwealth governments are contemplating these possibilities, with some moves in this direction – but power sharing is a stretch for government officials, and the public wants clarification of the rules of engagement before it can trust the process. Public consultation and participation in policy-making is sometimes referred to as electronic or digital governance. The premise behind the use of this term is that the outcome (the process of governance) is becoming more important in the public mind rather than the means of accomplishment (i.e., governments). Be that as it may, the instruments for delivering public services are still organised governments, so even e-government is just another project in the public forum.

Whichever phase of e-government a country is in, the key variable in successful technology transfer is operator training[20]. No country is immune to this requirement, regardless of its type of government or form of political culture. However, because of their democratic ethos, Commonwealth countries are better positioned to achieve an alignment between technology systems and political needs through the mobilisation of operator 'buy-in'. That is why technology transfer must be factored into the process of building e-government right from the beginning of project planning. There is no single 'right way' to design or implement e-government – it all depends on what the country needs and the trajectory of its political aspirations.

Reflecting this diversity of possibilities, academic analysts are taking a broad view of e-governance alternatives. The DigitalGovernance.org Initiative is a project of the London School of Economics in the UK[21]. It is aimed at studying, designing and propagating e-governance models. These models of e-government are generic, and include the following:

- a broadcasting model (disseminating information to the public);
- a critical flow model (informing the public of important issues);

- a comparative analysis model (benchmarking government performance);
- an e-advocacy model (mobilising the public, lobbying for action); and
- an interactive-service model (facilitating public participation).

As can be seen, these models summarise both the history and the alternatives of e-government. And depending on which choice, or combination of choices a Commonwealth government makes regarding e-government, the design of the system and the kind of technology transfer needed to support it will differ.

Conclusion

Commonwealth countries have had a wide range of experience to date regarding their decisions to adopt e-government, and they face a diversity of choices as they contemplate the future of their e-governance capabilities. How they will deal with these choices depends on their approaches to **benchmarking** (comparing other projects), **best practices** (identifying the best alternatives), and **technology transfer** (training the operators properly). Because e-government and e-governance are developing fields rather than co-modified products, there is no one right way to do things, nor one single goal towards which to strive. That is why the Commonwealth tradition of mobilising support and building consensus will still be the most effective basis to continue moving forward with electronic government.

Notes

1. Alan Freedman (2001).
2. Davenport and Prusak (2000).
3. DeLong (2004).
4. Turner (2002).
5. Ibid, pp.6–7.
6. eStrategies Online (2005).
7. Kovai (2005).
8. School of Computing (Middlesex University) (forthcoming).
9. Government of Victoria, e-Government Resource Centre, http://www.egov.vic.gov.au/ [accessed 1 February 2008].
10. Seifort (2003).
11. Vestel (2005) p.68.
12. Hiebler, Kelly and Ketteman (1998).
13. European Commission, *eGovernment Good Practice Framework*.
14. University of Manchester's Institute for Development Policy and Management, e-Government for Development, available at: http://www.egov4dev.org/ [accessed 1 February 2008].
15. Ibid, Topic 5: *Achieving Success/Avoiding Failure of e-Government Projects*, available at: http://www.egov4dev.org.topic1.htm [accessed 1 February 2008].

16. Roy (2006).
17. Perri 6 (University of Birmingham) (2004).
18. Bounfour (2005).
19. Gurstein (ed.) (2000).
20. Strassmann (1999).
21. London School of Economics, *DigitalGovernance.org Initiative*, available at: http://216.197.119.113/artman/publish/index1.shtml [accessed 1 February 2008]

3

From e-Government to e-Governance

Differentiating the two concepts

'E-government' and 'e-governance' can be defined as two very distinct terms. 'E-governance' is a broader topic that deals with the whole spectrum of the relationship and networks within government regarding the usage and application of ICTs. 'E-government' is actually a narrower discipline dealing with the development of online services to the citizen, more the 'e' on any particular government service – such as e-tax, e-transportation or e-health. E-governance is a wider concept that defines and assesses the impacts technologies are having on the practice and administration of governments and the relationships between public servants and the wider society, such as dealings with elected bodies or outside groups (not-for-profit organisations, NGOs or private sector corporate entities, for example). E-governance encompasses a series of necessary steps for government agencies to develop and administer to ensure the successful implementation of e-government services to the public at large. The differences between these two important concepts are explored further in this chapter.

The basis of the service

E-government is an institutional approach to jurisdictional political operations. E-governance is a procedural approach to co-operative administrative relations, i.e. the encompassing of basic and standard procedures within the confines of public administration. It is the latter that acts as the lynchpin that will ensure success of the delivery of e-services.

The 'e' part of both e-government and e-governance stands for the electronic platform or infrastructure that enables and supports the networking of public policy development and deployment. It is by now widely acknowledged that the original impetus for acquiring and using electronic apparatus in government and governance arose from earlier successes with the same kind of strategy in commerce. E-commerce had previously rested on credit and debit card processing for purchases, and on faxing of bulk orders and subsequent invoices in business-to-business transactions. In Canada, the United States and the United Kingdom, for example, the emergence of e-commerce by the private sector helped to stimulate and drive the evolution of e-government within departments and agencies. At the political leadership level, it was clear that

e-commerce was reflecting the enormous changes taking place in the economies of countries in the developed world.

The transformation of the Internet from an academic research network to a publicly accessible information utility prompted increasing numbers of businesses to create a 'web presence'. The initial postings were mostly electronic advertising brochures and product catalogues, with invitations to 'order by phone'. As e-commerce came to the fore, it became apparent to governments that customer expectations were moving in the direction of greater speed and convenience for transactions; so direct ordering through the Internet was developed and launched. The only issue that still inhibits the public from taking full advantage of e-commerce, is the concern with security of information and funds, a challenge that is also reflected in e-government and e-governance.

The success of e-commerce encouraged governments to recognise that citizens were now able to undertake transactions online and they were also capable of using email as an important communications tool that sped up and changed the way they communicated with each other. The evolution of the World Wide Web in the early 1990s created expectations that if businesses and the population at large could engage in online commerce and share knowledge and information in ways never before conceived, then it was incumbent on governments to provide online services. This phenomenon was a case of governments having to respond to a cultural change in the way people dealt with each other and with groups in society on an international basis. The high expectations of change resulted, by the mid-1990s, in rapid development of e-government services.

In essence, because the public liked e-commerce when it worked properly, they began to want their governments to perform in the same way. In terms of services provided, e-government and e-governance developed along the same trajectory as had e-commerce previously. The internal operational aspects of e-commerce included rationalising supply chains and business rules. This aspect was referred to as 'back office' requirements in government, and it focused around more effective workflow and information sharing.

The external offerings of e-government and e-governance started with making policy documents available electronically. Both 'stand-alone' studies and ongoing series (newsletters, press releases etc.) were posted and could be printed out as hard copies or stored electronically by whoever in the public was accessing them. The second phase of electronic products and services consisted of online electronic forms, either to exchange information (census forms etc.) or to conduct transactions (to purchase documents, pay user fees, submit tax returns etc.). The third phase, now just emerging, involves consultation on issues of concern, and participation in policy-making and regulatory administration.

The point of the above mini-history is to demonstrate that, in terms of the electronic platform and its operations, there are parallels between electronics for governing and e-commerce, and between e-government and e-governance. The computers, cables, software languages and communications protocols are all standardised products for any

kind of electronic networking, regardless of its information content or organisational context. What differentiates e-commerce from electronic governing, and e-government from e-governance is the purpose and functions that such networking supports. E-commerce is premised on profitable transactions, whereas e-government provides public services and e-governance facilitates appropriate behaviour. So, in each case, the motivation and the mandate will be distinct.

E-government as better public service

The observation has become accepted amongst government analysts that the public expects more and more in terms of service coverage and customisation, while at the same time expecting to pay less and less for such services in terms of unit costs (and the aggregate tax bill). This consideration is behind the decision to put an increasing proportion of government documents online – electronic distribution places the cost of paper and printing on the consumer rather than the supplier, and in the case of government documents this accounts for the biggest share of the price of making these documents available. It also takes far less time and person-hours to design and post an electronic document than to print and mail out the same information.

Electronic forms are also premised on lower costs and more convenience. Many jurisdictions enable driver's licenses to be applied for or renewed online. Use of such things as publicly provided recreational facilities can also be booked (reservations) and paid for (user fees) via government Internet websites. Even when some kinds of special reports are made available online, access to them may still be by subscription or single payment. Background budgetary documents, expert studies or reports from commissions of enquiry may all have charges attached to them, depending on the government's dissemination policy and the costs of preparing the documents. When there is a price attached, governments have set up e-commerce arrangements for credit-card payments similar to those that prevail in the marketplace.

The exchange of information between governments and various segments of the public similarly occurs increasingly by way of electronic forms. Businesses report many of their financial and functional operations to their governments via the Internet as part of their regulatory requirements. Data on the kinds, volumes and revenues of transactions go to the government's statistical repositories, to the finance departments for taxation purposes and to the particular departments that oversee the kind of business being conducted (automobile production figures go to the department for transport, for example). Those of the citizenry who are recipients of welfare and social assistance services (whether they be individuals or organisations) frequently use government websites and email to exchange information and file claims. By these means, governments check on eligibility, inform claimants on the terms and conditions of support arrangements, and provide training or instructions on such matters as job searches and income management.

The 'final frontier' of e-government is the attempt at extending 'e-democracy'. Voting has been conducted online, and will likely be extended once the design of the

user-interface has been rendered more 'user-friendly' and the security of the information has achieved more credibility. Consultation on issues of concern has been widely practiced, but with mixed results. The difficulty in this case is with clarifying the terms of engagement. There are three alternate formats available: (1) 'Tell us what you think/feel' merely asks for public input without any promise of either reporting back on that input or using the substance of the suggestions; (2) 'Share your views' carries the promise to at least report back to the public the transcript of what was provided as advice, with or without comments as specified in advance; and (3) 'Let's co-operate' involves the specific commitment to not only report back, but to actually use public input, or to explain in convincing terms why it is not to be used. The driving forces behind all of these developments will continue, as will the digitising of governments.

E-governance as co-ordinated propriety

The very concept of e-governance faces a dilemma: on the one hand, infractions of both legal requirements and good standards of behaviour have prompted many to ask for greater scrutiny and more stringent enforcement; on the other hand, over-controlling through draconian statutes or proliferating regulations, has a stagnating effect on management decision-making and organisational innovation. Good governance in general, and e-governance in and between large institutions and governments, is seen as a way to avoid the aforementioned shortcomings and still produce better outcomes.

Even the technical platform for some of this co-ordination has proven to be problematic. Information sharing, knowledge sharing and jurisdictional co-operation (horizontality), are the means to achieve e-governance. The previous arrangement of jurisdictional 'stovepipes' was (and is) the problem, but overcoming this problem has not proven easy. Once information, knowledge and jurisdiction are shared, the old notion of bureaucratic control and accountability is jeopardised. The only effective response to this challenge (if the co-operation is to succeed) is to re-conceptualise the situation as 'multiple contributions to common processes and solutions'.

Within governments, this e-governance will take such forms as these: shared databases of constituent particulars will assure consistent profiles are built and used so that services can be customised and repetitive data requests kept to a minimum (most constituents hate being asked for the same data by each department or branch). Where programmes or policies involve inputs from a variety of departments or branches, a single point of entry ('one-stop-shopping') can be arranged by creating a joint website that blends all of the requirements from the multiple sources, and presents it to the public as a unified programme or policy. In most cases, the users do not care where the inputs come from or what jurisdictional co-ordination was involved in producing the services – they just want the results to be convenient, high quality and low cost.

Between levels of government (national, provincial, municipal etc.) the mechanics of co-operation and co-ordination are even more challenging. From the public perception, a problem or issue as they see it may involve policy responsibilities and fiscal

implications from two or more jurisdictions. The planning, financing and maintenance or roads, the provision of health or education services, the regulation of land, water and air use, are all shared jurisdictions – but the public wants workable answers rather than excuses for persisting problems. However, this desire by the public for efficacious solutions does not alter the fact that co-operative arrangements have to be carefully thought out and diplomatically negotiated. The machinery of government does have hidden, long-term implications that may come back to haunt those who act too precipitously under the threat of public displeasure.

The e-governance solution to the handling of these diverging expectations is, ironically, both the most effective and the most disquieting to many public officials. Transparency is the one policy that expanding government networks can easily support. It can also shift the locus of contention away from public officials and onto disputing social factions. If consultation and participation are made transparent, the diverging values that cause policy conflicts can be revealed to be in the public domain rather than in the machinery of government. However, what this clearly leads to is the sharing of power with the public and other jurisdictions, to reflect their growing interdependence. As the scale, scope and complexity of situations and circumstances increases, this trend in e-governance will intensify.

4

Implementing e-Governance and e-Government

Assessment of readiness

E-governance is a dominant concept that is efficiently driving the implementation of e-government and technology projects around the world. The 'e' in e-governance refers to all aspects of technological implementation in governments throughout Commonwealth countries. The 'e' is also now referred to in multiple ways in the sense that it can refer to e-consultation, e-readiness, e-participation, e-delivery, e-performance or any computations and combinations referring to governance and programme implementation. It is important to stress at the beginning of this chapter that the ways in which e-governance is used are manifold. Implementing an e-programme in a developed country is far different than doing so in a smaller developing country that has limited financial or personnel resources. It is important that all implementation schemes take into account the possibilities and limitations that exist to get programmes up and running. Articulated below are the varying dimensions of e-governance and how the basic principles work for countries at different levels.

Definitions and nomenclature and the application of terms connected to any project being undertaken is important. As was explained above, e-government and e-governance can be defined as two very distinct terms. E-governance is 'a broad topic that deals with the whole spectrum of the relationship and networks within government regarding the usage and application of information and communication technologies (ICTs)', while e-government is 'a narrower discipline dealing with the development of online services to the citizen, more the 'e' on any particular government service – such as e-tax, e-transportation or e-health' (see chapter 3, above).

Developed countries have the financial and personnel resources to move forward quickly and efficiently in the evolution and implementation of online services. In fact, many countries, during the nascent era of e-government in the early- to mid-1990s implemented programmes that resulted in failures in bringing services online, which cost governments hundreds of millions of dollars. However, countries in the English speaking world, such as the United States, the United Kingdom, Canada and Australia, when confronted with overspends, were able to absorb the losses and move on to develop online services with sufficient funding and the necessary personnel for projects. However, when considering e-government implementation in developing countries a different approach is needed. Essentially, many of these countries have been able to

turn to donor international organisations and developed countries for finance and personnel resources.

Putting the 'e' on services, such as e-health, e-participation, e-voting, e-environment or e-weather, for example, serves as a guide to the wider subject matter of e-government and e-governance, which can, in time, be imprinted on the public mind. More importantly, the use of terms such as 'e-government', 'e-governance' and 'e-democracy', leads to the creation of an identifiable discipline. This then widens the development of the subject beyond the parameters of government alone and to the larger spheres of civil society, associations, unions, the business community, international organisations and the academic world.

In society, it is the identifying of concepts through words and phrases that leads to cohesion and order. Subject matters create an ambience between stakeholders throughout the society. For example, 'public transportation' or 'environmental issues' are phrases understood by citizens who then relate them in their minds to the mass movements of our times. This is the way e-government must continue to evolve.

In time, technologies will change the way society shapes itself, and this will lead to a widening of the subject matter into new spheres. At that point, a new nomenclature will arise reflecting the change articulated in future generations. However, this new nomenclature will only be an extension of the discipline that began to evolve in the late 20th century. The danger in this time of modernity is the urge to move with the latest 'craze' or 'fad'. It is the job of governments to maintain stability at times of great change, such as those in which we are now living. Part of this stability involves forward thinking while keeping rooted in acceptable principles and processes. Government, governance and democracy have been with us for a long while. By adding the 'e' to these words we maintain a stream of thought and a conceptual framework with which the public can relate. Governments are not in the business of creating fads. Many international organisations have come to accept these terms, and they and other respected thinkers and authors are contributing to this important process of change.

E-government programmes are now 'citizen-centric' in that governments conduct in-depth surveys to determine what particular services take first priority. For example, in some countries, such as Canada, an early innovation was the implementation of online filing of tax forms. Over the years this and other online services have proven to be successful across all sectors of society. A 'citizen-centric' approach to e-government recognises that the needs of the citizen come first and will result in successful implementation of online services. In many countries, citizens take for granted the right to go online and engage in information gathering or communication via email or through government websites to public servants. Government websites around the world are now vast information repositories.

Citizen-centric government

Research looking at the activities of many governments and international organisations around the world indicates that much has been done, and continues to be done,

to move into this new form of online governance. Governments on the whole are aware of the changing expectations of their citizenry, and of the desire, especially by not-for-profit groups and emerging e-democracy groups, to have a say in the evolution of government policy. How governments deal with this could very well determine future relationships between government and the citizenry. This is a serious governance issue that many governments are now facing. For example, the UK government has evolved extensive e-participation programmes at the national and local level, allowing citizens to engage in dialogue with government departments. This is happening globally, as not only governments but many 'e-democracy' groups have emerged in many countries, developing tools, resources and programmes to involve citizens in the fast growing e-democracy movement worldwide.

E-government continues to be implemented throughout the Commonwealth through a series of important actions. These include political leadership and input of senior public servants, cross-government departmental co-operation, working partnerships with the private sector, especially in the IT sector, and consultation with citizens and groups in society. The latter can be achieved through a number of mechanisms, such as surveys and focus groups, in order to determine what members of the public want in terms of online services.

It must be stressed here that there are vast differences in the implementation of e-government in developed and developing countries. For example, some key elements of success in developed countries are sufficient, experienced and professional personnel equipped with:

- funding;
- resources;
- political support; and
- the ability to build technology infrastructures.

The five points to be implemented to assure the evolution of e-government projects and initiatives in developing countries are:

1. Political approval of funds and resources from a variety of international organisations;
2. Leadership at the top echelons of government to see that e-government projects are implemented;
3. Sufficient financial and personnel resources;
4. Built-in policy issues, such as security, privacy and accountability; and
5. Committees from different levels of government or within departments co-operating to bring the concept e-government to fruition.

The majority of medium-developed and developing countries receive extensive funds to implement e-government projects. International organisations such as the World Bank, the OECD, the British Council, the Canadian International Development Agency

(CIDA) and the United Nations are just some of the donors. In some instances funding is on a lending basis, though sometimes there are programmes from international organisations providing the necessary funds as outright donations and grants. International organisations also often send experts and consultants to developing countries as advisers for the evolution of IT and e-Government programmes.

An important route to success for developing countries is the development of national IT plans. These are essential to assure success, because they allow for inclusion of all the different aspects of what needs to be done. An 'e-readiness' assessment plan is also crucial if the development of e-government projects is to be successful. For example, one of the first steps to be made when moving forward with IT projects to service the public is to determine the number of households, educational institutes, government agencies and departments, and commercial organisations that have online capacities through which online services can be offered. This will determine the number of services to go online and what funding and personnel are needed. An assessment as to what priority to give each of the services to be implemented must also be made.

An essential point to be made about the evolution of e-government in developing countries is that the circumstances vary from country to country. In many jurisdictions, e-government services would only be available in major cities, because in smaller jurisdictions and towns the necessary infrastructure is not there to bring such services. When there is no Internet connection or facility to hand, mobile phones become the technology of choice to access government services online. Mobile phones have been made available at low cost or as donations in many countries. While this is a solution to gain access to government services, the fact remains that in many poor countries there are too many people that do not have access to these services.

E-governance and e-government are now institutionalised programmes in the majority of countries around the world. There is a large grouping of materials on these subject matters online and in the halls and libraries of governments, universities, NGOs, consulting firms and a host of other groups in society. At the time of writing, only about a sixth of the world's population has some form of online access, even though 94 per cent of countries have some form of online infrastructure. There are many challenges that lie ahead to encompass the poor and disenfranchised of the world. E-governance and its sister groupings can help to bring the information richness of the online world to more and more people. We are at a stage of fundamental change in which the Internet and other new technologies are changing our cultures and the way we live. Our biggest challenge for the future is to encompass more of the citizens of the world in that change.

The following chapters largely report on the context, contents and conclusions of the workshop entitled the Regional Workshop on e-Government Readiness for Effective Public Service Delivery (4–8 June 2007), which was developed by GIDD of the Commonwealth Secretariat, supported by the Government of the Cayman Islands, and was held in Grand Cayman with participation by the countries of the Caribbean and the Mediterranean.

5

Electronic Government in Barbados and the Caymans

The context of the workshop

Prior to the Commonwealth Secretariat Regional Workshop on e-Government Readiness for Effective Public Service Delivery (4–8 June 2007), the governments of both Barbados and the Cayman Islands had already adopted e-government on a department-by-department and a programme-by-programme basis. Websites and email were provided for select services, the purpose of which was to assist the general public and the business community. These 'start-up' projects were developed on an individual basis, because this strategy best reflected the limited resources and experience available at the time.

As a result, there were no 'master plans' or generalised implementation criteria for e-government in these locations prior to 2007. Nevertheless, it is still possible to get a 'state of the art' profile of Barbados's e-government accomplishments by referring to the assessment of the Caribbean Technical and Advisory Support Facility (TASF) on e-Government, prepared by the United Nations Department of Economic and Social Affairs (UNDESA) and the Caribbean Centre for Development Administration (CARICAD). This profile, which the authors reproduce in what follows, is presented on a publicly-accessible website[1].

BARBADOS

TASF's profile of Barbados (as of 2005)

This first section of the profile deals with the categories of available electronic services.

Table 5.1 Technical and Advisory Support Facility: profile of Barbados and available electronic services (2005)

Topics / solutions in Barbados	**e-government stages (solutions)**	Additional comments
Public policy	n/a	
Country strategies	n/a	The National Strategic Plan of Barbados 2005–2025, available at: http://www.barbados.gov.bb/Docs/NSP_Final%202006-2025.pdf [accessed 4 February 2008] Draft National ICT Strategic Plan, available at: www.commerce.gov.bb/Downloads/DRAFT_StrategicPlanFinalV.pdf [accessed 4 February 2008]
Networks interoperativity	n/a	
Electronic signature infrastructure	n/a	
Electronic certificates and digital signature legislation	n/a	The Electronic Transaction Act is in place and the regulations giving effect to this Act were being drafted at the time of writing. The Act makes provision for the establishment of a legal environment for the conduct of electronic commerce. See: www.commerce.gov.bb/Legislation/default.asp [accessed 4 February 2008]
Topics/ solutions **in Barbados**	**e-government stages (solutions)**	**Additional comments (indicate URL)**
e-commerce legislation	n/a	The Electronic Transaction Act is in place; the Data Protection and the Computer Misuse Act were being drafted at the time of writing. See: www.commerce.gov.bb/Legislation/default.asp [accessed 4 February 2008]
Electronic fraud legislation	n/a	The Computer Misuse Act makes provision for the protection of computer systems and information contained in those systems from unauthorised access by individuals or from abuse by individuals with authorised access and for related matters.
Habeas data legislation	n/a	
Other legislations (please specify)	n/a	The Government of Barbados was considering the introduction of a Freedom of Information Act at the time of writing. A draft policy document, which offers guidance on a freedom of information regime, has been prepared; this document was being circulated for comments at the time of writing.

The above section lays out the general framework within which a country's readiness for the further application of e-government can be assessed. As can be seen in the case of Barbados, some areas already have an e-government capability, some are in the process of developing such capabilities, while other aspects of government have not yet been addressed.

The next section of the profile classifies individual electronic services according to the e-government stages they have achieved.

Table 5.2 Technical and Advisory Support Facility: profile of Barbados and classification of individual electronic services (2005)

Available services in Barbados	**e-Government stages (solutions): I Informative II Interactive III Transactional**	Additional comments
Tax declaration	**I**	Inland Revenue Department, available at: www.barbados.gov.bb/ird/ [accessed 4 February 2008]
Government procurement		Smartstream Product Suite includes **Smartstream Procurement**, made up of payables and purchasing modules. This application has been fully implemented.
Accountability		
Property rights registration	**II**	The Corporate Affairs and Intellectual Property Office has a website where the public can view relevant legislation, download forms and search for registered companies, charities or business names. Available at: www.caipo.gov.bb [accessed 4 February 2008]
Payroll management		Smartstream Product Suite includes **Smartstream Human Resources**, of which payroll and personnel modules have been implemented.
Available services in Barbados	**e-Government Stages (solutions): I Informative II Interactive III Transactional**	Additional comments
Social welfare	**I**	The Ministry of Social Transformation has a website, which informs the public of the various services it offers. See: www.socialtransformation.gov.bb [accessed 4 February 2008]
		The Ministry of Social Transformation also has responsibility for the Community Technology Programme. This programme is geared towards ensuring

		that communities/individuals have the ability to acquire basic skills in ICT and access to the Internet.
Promotion of exports and competitiveness	**I**	The Barbados Investment Development Corporation has developed a website to assist the department in fulfilling its mandate to promote and facilitate the establishment and expansion of business and the export of goods and services.
Financial management		Smartstream Product Suite also includes **Smartstream Financials**, which comprises ledger, funds control, accounts receivable and budget modules. This applica tion has been fully implemented.
Civil registry management		An Electronic Document Management System is in use at the government's Registration Department. This application captures the image of original vital statistics records and automates the functions associated with the registration of births, deaths, marriages, wills, probate applications and the processing of certificates.
Land Registry management	**III**	The Land Registry was due to launch its website and online billing **(Platypus)** system at the time of writing. This online billing facility will enable the department to charge for virtually any type of data and in a variety of billing methods, including according to time periods, usage, day, bandwidth and even prepaid 'blocks'. The Platypus online billing application will also be capable of automatically sending invoices for charges incurred, as well as permit the creation of notices required to be sent to customers based on characteristics that include soon-to-expire services and 'funds declined' notices, to name a few. An Electronic Land Register will also soon be in place. This application permits an adjudication record to be created and automatic creation of the Land Register. Website available at: http:// www.landregistry.gov.bb [accessed 4 February 2008]
Public transportation management	**I**	The public bus company (Transport Board) has a new ticketing system, the **Wayfarer Ticketing System**. This system utilises an integrated software package, which allows the board to generate reports to facilitate wide-ranging management decisions. In addition, it gives the board the opportunity to closely monitor 'ridership' patterns and as a result increase its operating efficiencies as they relate to productivity, allocation of routes and disbursement of buses, while also improving the productivity of ancillary departments. Website available at: http://www.transportboard.com/ [accessed 4 February 2008]

Country's general statistics		
Available services in Barbados	**e-government stages (solutions): I Informative II Interactive III Transactional**	Additional comments
Public records available online		The public can download information and access other government websites through the government portal at: http://www.barbados.gov.bb/ [accessed 4 February 2008] Information can also be obtained from the Government Information Services website, available at: http://www.barbados.gov.bb/bgis.htm [accessed 4 February 2008] There is a project underway to replace this site with an integrated portal, which will be an electronic gateway to the government's information and services. A pilot has been successfully completed and funds have been approved for full implementation.
Promotion of exports and competitiveness	**I**	The Barbados Investment Development Corporation has developed a website to assist the department in fulfilling its mandate to promote and facilitate the establishment and expansion of business and the export of goods and services.
Legislative power online		
Records management		
Municipal administration		
Electronic voting		
Geographic information systems		The Government's Land and Surveys Department is planning to introduce a digital mapping system utilising ESRI GIS (geographic information system) software. At present, the department is undertaking a digital mapping programme, which will form the basis of the GIS system.
e-learning in public schools	**II**	The government has embarked on a comprehensive education reform programme (Edutech) in the primary and secondary schools in Barbados to integrate all available information and communication technologies within the school system. Additional information can be obtained from the Edutech website:

		www.edutech2000.gov.bb [accessed 4 February 2008] The Samuel Jackman Prescod Polytechnic, a training/ vocational training institution in Barbados, has launched an online learning facility and is currently offering courses online. See: http://www.sjpponline.edu.bb/ [accessed 4 February 2008]
e-democracy	**II**	The Parliament of Barbados has a website that the public can access, available at: www.barbadosparliament.com

As these examples from the TASF profile show, there are many e-governance and e-government initiatives underway in Barbados, all at various stages of development. Some of the examples also indicate the intention to upgrade existing services in the immediate or foreseeable future.

There is no Barbados Government Gateway website, nor does the Barbados Government Information website provide a list of the individual websites referred to above. However, some sense of what the Government of Barbados intends with respect to e-government can be gleaned from The National Strategic Plan of Barbados 2006–2025. The relevant sections of the Plan are provided below:

Social objective 2.4: To remodel the public service

EXPLANATION:

A streamlined, efficient and professional public service is absolutely essential for our continued development.

STRATEGIES:

2.1 Ensure that in the new paradigm of governance there is a better fit between the tasks of government and the way in which the public service is structured.

2.2 Promote greater openness, transparency and accountability in the operations of central government, as well as in the operations of public enterprises.

2.3 Facilitate the sharing of information and the quick and easy access to information throughout the public sector and access to information for the private sector and civil society organisations.

2.4 Remodel various aspects of the public service to reduce bureaucracy and increase efficiency and effectiveness through performance-based initiatives.

2.5 Integrate modern information and communications technologies into the operations of government to facilitate maximum operational efficiency.

2.6 Promote the development of a more customer and service delivery oriented public service.

2.7 Build the human resource capacity within the public service to allow it to operate at maximum potential.

2.8 Ensure that the public service has the human resource capacity and appropriate organisational structures to facilitate the efficient and effective attainment of national goals.

2.9 Reform the multi-processes across the public service to create an efficient and time effective sector.

Targets:

2.1 The enactment by 2007 of the Public Service Act which will be designed to encourage modern management practices and to develop a culture of openness, transparency and accountability in the public service.

2.2 The creation of the Central Information Management Agency by 2008 to champion the government's e-government strategy and programmes, which will be geared at ensuring the optimum use of information and communications technology to achieve maximum operational efficiency in the public service.

2.3 The development of a mandatory strategic training programme for the public service by 2008.

2.4 The establishment of ten-customer charters in public sector agencies through consultation with stakeholders by 2008.

2.5 Elimination of multi-processes across the public service by 2010.

2.6 Introduction in all ministries by 2010 of a revamped performance management system which appraises the performance of employees on objective and measurable work outputs.

2.7 The development by 2010 of a manpower resources plan for the public service that identifies the appropriate human resources required to meet national goals in the most efficient and effective manner.

2.8 Completion of organisational reviews of each ministry by 2015 to ensure that existing structures are appropriate to the attainment of organisational goals.

Fiscal objective 1.1: To develop a transparent and sustainable public finance management system

Explanation:

The purpose is to promote efficiency and effectiveness in the current tax collection systems as well as the system of expenditure management. This would enhance financial stability and sustainability, improve compliance, reduce tax leakages and increase the level of tax revenue collection.

STRATEGIES:

Tax administration system

1.1 Undertake institutional strengthening and capacity building of the overall revenue collection systems, which will include the design of a new tax administration system for the Inland Revenue Department, the VAT Division and the Land Tax Department.

1.2 Develop e-government services with the aim of creating an enabling environment that would enhance the efficiency and effectiveness by which business transactions can be undertaken between members of the public and relevant government agencies with regard to the administration of the tax system.

1.3 Upgrade and modernise the various tax collection agencies, namely the Inland Revenue Department, the Land Tax Department, the VAT Division and the Customs and Excise Department. This will be done by undertaking a revision and automation of the current administrative processes at the various agencies and introducing new technologies and processes to bring the current systems in line with internationally recognised tax administration 'best practices'.

1.4 Undertake the automation and modernisation of the non-tax revenue departments, such as the Corporate Affairs and the Licensing Authority, to enhance the collection capacity of these institutions.

1.5 Give consideration to the establishment of a Central Revenue Collection Authority, to remove the administrative fragmentation that currently exists in the system.

Objective 1.2: To ensure easier access and use of telecommunications

EXPLANATION:

For Barbados to launch itself completely into the information age, the development of and access to telecommunications is a key stepping-stone. This requires having the physical infrastructure for telecommunications capable of responding to the technological challenges of the 21st century.

STRATEGIES:

1.1 Strengthen the linkages between telecommunications and the other sectors of the economy.

1.2 Promote access to basic telecommunications and information services. This may be accomplished through further community-focussed initiatives, through wider coverage in the education and training systems and through the promotion of technology-based businesses, such as Internet cafés.

1.3 Promote the development of telecommunications, and other information communication technologies (ICTs).

1.4 Promote the development of e-commerce, e-government and e-business.

1.5 Facilitate greater competition, development and innovation in telecommunications in order to expand the range of services and to increase value for money in the sector through reduced costs to consumers.

1.6 Improve the institutional and human resource capacity of the telecommunications sector.

1.7 Invest in and encourage the development and expansion of the physical infrastructure of telecommunications through enhanced satellite uplinks and other digital media.

CAYMAN ISLANDS

Profile of the Cayman Islands from the government website

There is no Cayman Islands e-government profile available from the TASF. Enquiries indicate that, at the time of writing, there was no centralised website for e-government in the Caymans. However, there is a general Cayman Islands website, and this includes a sub-section that lists existing Cayman Islands Government websites. By listing those available websites in a table, it is possible to get an idea of what the various government departments are doing in this regard. The Cayman Islands' civil service is, in fact, working on increasing access through e-government, but prior to 2007 each agency had been heading its own projects.

Table 5.3 Existing Cayman Islands Government websites

Cayman Islands Government websites[2]	*Website descriptions*
Blue Iguana Recovery Programme	Devoted to raising awareness of the Blue Iguana as an endangered species, and to promoting recovery measures
Boatswain's Beach	Information on Boatswain's Beach Park on Grand Cayman
CINICO	National Insurance Company website providing information and application forms
Civil Aviation Authority	Website of the aviation regulatory oversight board
Civil Service College	Forms, materials and log-in capability to the College
Cayman Airways	Flight schedules and booking facilities
Cayman Islands Customs	Customs forms and import/export restrictions
Cayman National Cultural Foundation	Cultural events and facilities on the Caymans
Cayman Prepared	National Hurricane Committee website
Civil Service Appeals Commission	Information on the adjudication of Civil Service personnel disputes
Communications, Works and Infrastructure	Promotes infrastructure for community development
District Administration, Planning, Agriculture and Housing	District planning and implementation of infrastructure projects
Dive Cayman	Website for bookings for diving excursions
Economics and Statistics Office	Data to serve the needs of local community and international investors
Ministry of Education, Training, Employment, Youth, Sports and Culture	Information on programmes for learning, working, and leisure activities
Education Portal	Access to information on the entire range of primary and secondary school facilities

Cayman Islands Government websites[3]	*Website descriptions*
Elections Office	Returning Officer's website and listing of election results
Employment Relations	Promotes labour relations and training opportunities
Environment	Promotes environment and natural resources conservation
Finance and Economics	Departmental site with information on macroeconomic and budgetary policies
Financial Services	Information on the Cayman financial services industry
Freedom of Information	Preparing the public for pending freedom of information legislation
Health Insurance Commission	Helping the public to utilise their health insurance and resolve any complaints about it
Health Services Authority	A guide to inpatient and outpatient services
Immigration	Work permit information for Cayman Islands companies
Information and Communications Technology (ICT) Authority	Information from the ICT regulatory authority on policies and decisions
Internal and External Affairs	For co-ordination of legislation and policy application, within the country and abroad
Investment Bureau	Information for potential investors on Cayman opportunities
Judicial Administration	The Judicial and Legal information website
Lands and Survey	Geographical and geological information
Law School	The Law School calendar and course schedules
Legislative Assembly	Order of Business of the House of Assembly
Mosquito Research and Control Unit	Ground and aerial spraying schedules by area
Meteorological Office	Weather forecasting and information service
Monetary Authority	Information on exchange rates and currency trading
National Drug Council	Information and assistance on eradicating drug abuse
National Gallery	Exhibits from and schedule for the National Gallery
National Museum	Preservation, research and display of national heritage
National Pensions Office	Information on the regulation of private pension plans
National Roads Authority	Promoting the design and maintenance of Cayman roads
National Trust	Preservation of national historical sites
Nature Cayman	Guide to natural wonders in the Caymans
Office of Complaints Commissioner	Site to guide Cayman residents on registering any complaints about their government
Office of the Governor	Official website of His Excellency the Governor
Planning	Promotes planning that assures the quality of life
Port Authority	Information on port facilities and shipping schedules

Postal Services	Postal rates, postal codes and stamp collecting
Public Service Pensions Committee	Administration of public service pensions plans

Cayman Islands Government websites[4]	*Website descriptions*
Queen Elizabeth II Botanic Park	Park opened by Her Majesty Queen Elizabeth II
Radio Cayman	Broadcasting schedules and programme features from Radio Cayman
Recruitment	Website for recruitment of government personnel
Sister Islands Tourism Association	Arranging excursions amongst the Cayman Islands (Grand Cayman, Brac Cayman and Little Cayman)
Shipping Registry	Registration of vessels and regulations affecting them
Stock Exchange	Listing brokers, agents and issues
Tourism Attraction Board	Manages the country's top five tourist attractions
Tourism	Promoting travel to the Caymans
University College	The Caymans institution of higher learning
Water Authority	Providing safe and inexpensive drinking water to the public
Women's Resource Centre	Addressing the needs of women in the Caymans

There is indeed a proliferation of Cayman Islands Government websites, with a wide variety of information and services to the public and the business community. Two illustrative case studies follow.

Case Studies of e-government in the Cayman Islands

The Department of Communications, Works and Infrastructure is responsible for the building, operation and maintenance of all Cayman publicly-owned equipment and facilities. These public goods are the basis of the quality of life and key to development of the community and the country. The Department's website covers the Ministry's mission statement, subjects (areas of jurisdiction), ambit of the vote (policy framework), review of 2000 achievements and key objectives for 2001.

Department of Communications, Works and Infrastructure: Mission Statement:

'To promote a sustainable, high quality of community life, to keep pace with the level of economic development and changes in the Islands, and to ensure that each individual has the maximum opportunity to achieve his or her highest potential level of self-fulfilment and personal development, in terms of the physical, social, moral and spiritual aspects of life'.

Subjects (areas of jurisdiction):

- Anti-Drug Abuse Programmes
- Care and Protection of Young Persons
- Community Development
- Ecclesiastical Matters
- Ex-Servicemen
- Prisons
- Housing
- Refugees (Welfare of)
- Social Development Services
- Sports and Recreational Facilities (fields and parks)
- Seamen
- Sewage Treatment and Sewerage Systems
- Voluntary Sports Organisations
- Water Distribution and Sales
- Water Resources Protection
- Women
- Youth (Organisations, Activities, Policy)

Ambit Of The Vote (policy framework):

'To formulate policies and support community activities; promote healthy lifestyles and provide financial benefits to eligible ex-servicemen and seamen, maintain sports and recreational facilities and programmes; formulate a Sports Policy, implement the National Youth Policy; and develop programmes to enhance the status of women and families; ensure the holistic implementation of community development in the three islands to keep pace with economic growth'.

Review Of 2000 Achievements:

1. Provided financial assistance to 512 ex-servicemen and 595 seamen
2. Revised the criteria for grants to community groups
3. Continued the process of developing a National Policy on gender and Gender Equity

4. Furthered developed and maintained the services, programmes and resource library at the Women Resource Centre by providing an administrative assistant and additional office space
5. The National Youth Policy was completed and submitted to the Legislative Assembly
6. Continued to provide after-school, youth workers and youth development grants to various churches and organisations

Key Objectives For 2001:

1. To continue to provide assistant to ex-servicemen and seamen
2. To commence work on a National Social Policy
3. To continue developing a National Policy on Gender and Gender Equity
4. To further develop and maintain the services, programmes and resource library at the Women Resource Centre
5. To develop plans for a 'Place of Safety' for victims of domestic violence
6. To develop an implementation plan for the National Youth Policy
7. To establishing a National Youth Commission, an independent body that will monitor the implementation of the National Youth Policy
8. To establish an inter-ministerial Committee on Youth

The Employment Relations Department is also a good example of website outreach – it provides a variety of necessary services to the community and the country. Some of the information from that website is listed below to show the department's public services.

Department of Employment Relations (ERD)

The Cayman Islands Government's Department of Employment Relations endeavours to develop a highly skilled, productive workforce that is able to compete effectively in the global economy. The Employment Services Centre's goals are achieved through advising, educating and training, promoting harmonious labour relations and ensuring that the rights and dignity of both employers and employees are protected.

ERD creates results for its clients by providing services in the areas of:

- Conciliation and mediation
- Inspection and compliance
- Job placement
- Human resource development
- Local and overseas scholarships

- Small-business development

The following hyperlinks are then listed through which the public can get relevant information:

- Training and Development
- Education Council
- Good Practice
- Investors in People
- Job Seeker
- Small Business
- Conciliation and Mediation
- Inspection and Compliance
- Occupational Safety and Health Information
- Download Occupation Wage Survey

Download Occupational Health and Safety Code of Practice for the Construction Industry.

Notes

1. Red de Líderes de Gobierno Electrónico de América Latina y El CaribeRed (GEALC), available at http://www.redgealc.net [accessed 4 February 2008]
2. Cayman Islands Government, website portal: http://www.gov.ky/portal/page?_pageid=1142,1595604&_dad=portal&_schema=PORTAL [accessed 4 February 2008]
3. Ibid.
4. Ibid.

6

Commonwealth Secretariat Workshop Report

Setting the framework for the workshop

Devindra Ramnarine of the Commonwealth Secretariat began the substantive portion of the workshop with a presentation of a holistic approach for national connectivity to narrow the digital divide[1]. This national ICT plan would involve community connectivity, training and human resource (HR) development, ICT industry development, e-government and proper legislation and infrastructure. The creation of the national ICT plan was depicted through figure 6.1, below.

The progression of steps is from left to right. The first step is to develop an information and communications technology vision and policy that encompasses stakeholders and their expectations regarding e-government. Next, e-readiness needs to be assessed based on standardised measurement methodologies. At the same time, a benchmarking exercise can be conducted to compare experience and best practices in e-government from other countries. Based on the results of the e-readiness assessment and the benchmarking exercise, any gaps that have been identified in a country's e-government

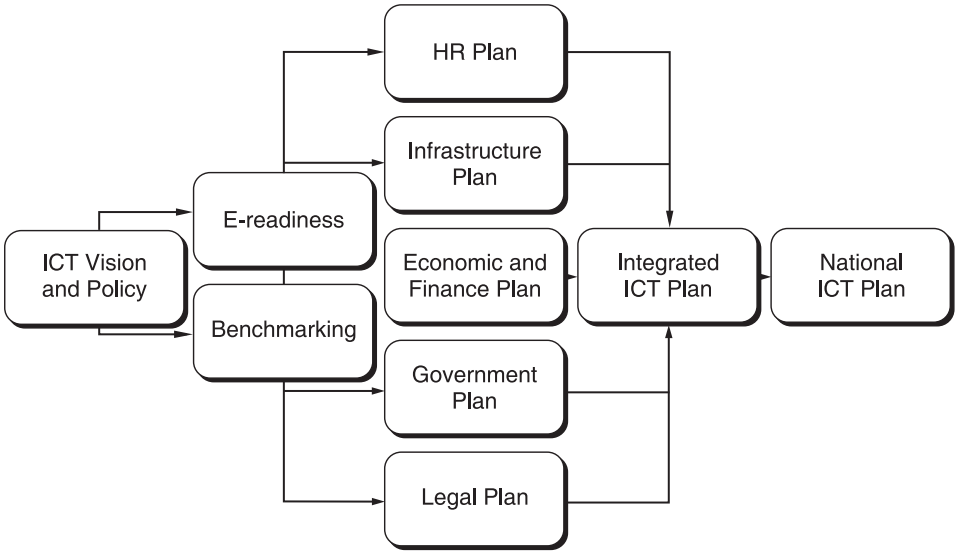


Figure 6.1 A holistic ICT policy for national connectivity

intentions with respect to its human resources plan, infrastructure plan, economic and finance plan, machinery of government plan or legal plan, can be addressed in the integrated ICT plan, which when effectively communicated to all stakeholders would become the national ICT plan for the country.

Mr Ramnarine cautioned about the need for national ICT plans to be implementable and not just rhetorical. Some existing policies might need to be revised, and funding arranged. All of this could best be done within a project management approach to assure that timelines were set, objectives met and risks ameliorated. He identified critical success factors as being (i) promotion of e-government by a sponsor; (ii) making the plan part of national development; (iii) achieving buy-in from stakeholders and managing change effectively; (iv) educating the public on the benefits of e-government; (v) procuring affordable technology; and (vi) providing leadership for e-government from within government itself. He also recommended that countries use the Commonwealth Secretariat's Commonwealth Connects Portal (www.commonwealthconnects.net) as a source of information about e-government best practices, the necessary legal framework, technical standards and so on.

Citizen-focused service and e-government[2]

A number of subsequent workshop sessions were then presented by Dr Albert Tan of Singapore. The rationale for Dr Tan's approach is the advocacy by the World Bank on the issue of public service delivery[3]. He began by defining the purpose for which e-government is adopted, namely for 'the integrated delivery of information and services by all levels of government to citizens, businesses and public organisations, through the application of information communications technology (ICT) for government transformation'. He illustrated his points using figure 6.2.

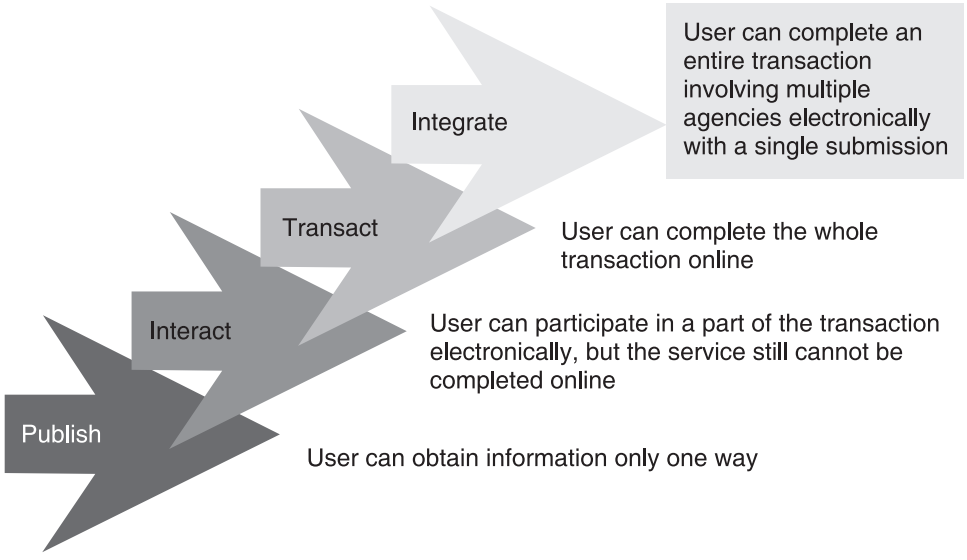


Figure 6.2 The purpose of e-government

Dr Tan reviewed the recent history of the spread of e-government, noting in particular that more and more services were moving online, and in the process that governments' relations with both their constituents and clients was changing. He emphasised that the transition to e-government was a continuous process rather than a short-term project. As a result, successive opportunities would present themselves for service extension, and governments should be ready to recognise and adopt these opportunities.

For instance, in government-to-business relations (G-B), e-procurement is the new business revolution that can help governments lower operational costs, empower aggregated cross-organisation spending, and gain unprecedented access to a global supplier base. The public sector can become a role model for e-procurement to catalyse the penetration of e-commerce into the private sector.

In a similar way, in government-to-citizen (G-C) relations, more and more citizens in Singapore are accessing their government services online. e-Citizen (a G-C portal in Singapore) is a first stop on the Internet for public e-services (online services). In the course of one year, the number of hits on e-Citizen increased from 240,000 to a few million hits per month. Going forward, a key focus of the public sector is to integrate public services across agencies to provide citizens with a single touch point or interface.

Government agencies in Singapore have made substantial efforts to make online government services simpler and more convenient to the public, and the number of government services delivered online increased over the year 2001 from 65 per cent to 90 per cent of all feasible services. The focus for Singapore today is in transformation of government services, rather than merely automating and digitising existing government processes as shown in the e-government maturity model.

Dr Tan concluded his presentation recommending that participants build e-government initiatives based on **outcome** measurements and avoid using **output** measurements only that might end up delivering e-government services that are not needed, resulting in user dissatisfaction and low utilisation.

Selecting e-government services[4]

In the session on selecting e-government services, Dr Tan highlighted the types of value propositions that can be derived from e-government: some are tangibles, while others are non-tangibles. Based on his experience, Tan asserted that tangible value propositions are easier to justify than the non-tangible ones. Government processes can be evaluated to match these propositions, with three criteria commonly used to justify selection being the cost, time and quality of service rendered. Processes that closely match the value proposition are selected for e-government implementation due to limited funding and resources. Examples of such value propositions are listed below.

Table 6.1 The value propositions that can be derived from e-government

FUNCTIONAL AREA	*Tangible value propositions*	*Non-tangibles value propositions*
Agency	❑ Faster business transactions ❑ Increased access to information ❑ Increased data integration across applications ❑ Fewer errors	❑ Stronger relationship with customer/citizens ❑ Enhanced responsiveness ❑ Better service ❑ Enhanced agency reputation
Information Services	❑ More effectively integrated systems ❑ Ease of support	❑ Increased system availability ❑ More satisfied end-users ❑ Availability of more accurate information to support data analysis activities
Acquisition	❑ Reduction of paper ❑ Reduction of manual effort ❑ Better information to make critical buying decisions ❑ Error reductions ❑ Reduced Inventory	❑ Fewer reorders due to discontinued items ❑ Stronger vendor relationships ❑ Cost reduction
Customer Service	❑ Reduce manual effort ❑ Reduce data entry ❑ Reduce paper process ❑ Reduce staff or avoid hiring more staff ❑ Move staff to more value-added jobs	❑ Faster, more effective customer support ❑ Lower burden on mailroom ❑ Reduced process steps facilitate faster processing of information
Finance	❑ Reduce discrepancies ❑ Reduce claims and adjustments ❑ Reduced data entry	❑ Process improvements in reconciliation of invoice, purchase order and remittance ❑ Reduced phone time/ improved efficiency
Administrative	❑ Reduce manual effort ❑ Reduce data entry errors ❑ Reduce paper process ❑ Reduce staff or avoid hiring more staff ❑ Move staff to more value added jobs	❑ Reduce redundancy ❑ Streamlined time to process information ❑ Accomplish more without additional hires

After this material was presented, the workshop participants were asked to list some value propositions for their country's e-government. Most participants listed value propositions that would mainly be relevant to citizens rather than those for business people or employees. Dr Tan advised them not to limit exploitation of e-government to citizens, but to expand further to include its use by businessmen, women and employees.

Re-engineering e-government processes[5]

The session on re-engineering e-government processes focused on the presentation of the concept of process and 'business process re-engineering' (BPR) to the participants and highlighted the importance of BPR for public sector reform. BPR was defined in the classical sense as 'the fundamental rethinking and radical re-design of business processes to achieve dramatic improvements in critical measures of performance, such as cost, quality, service and speed' as per *Re-engineering the Corporation* by Hammer and Champy, 1993.

Even though BPR started in 1993 and has been used extensively in the private sector, the concept has not seen much use in the public sector. The key motivations for BPR in the public sector are mainly cost reduction or compliance with new regulations. Another possible reason for the application of BPR may be due to some 'burning platform' that an organisation is 'standing on'. In that case, something has to be done fast before the 'platform' sinks.

Dr Tan explained the typical drivers for BPR in the public sector. These included:

- Reducing costs
- Improving customer service
- Increasing national competitiveness
- Improving operating efficiency
- Increasing capacity
- Ensuring compliance with new law or policy
- Meeting/anticipating crisis
- Exploiting new technologies

A video on BPR was shown to further explain some of the key success factors for BPR and change management. Tan concluded with a BPR framework (see below) for everyone to use for future BPR projects.

Managing implementation[6]

The 'managing implementation' session consisted of a group discussion on how to manage the implementation of e-government. Participants were formed into three groups and tasked to discuss on how they could replace an agency counter service with online

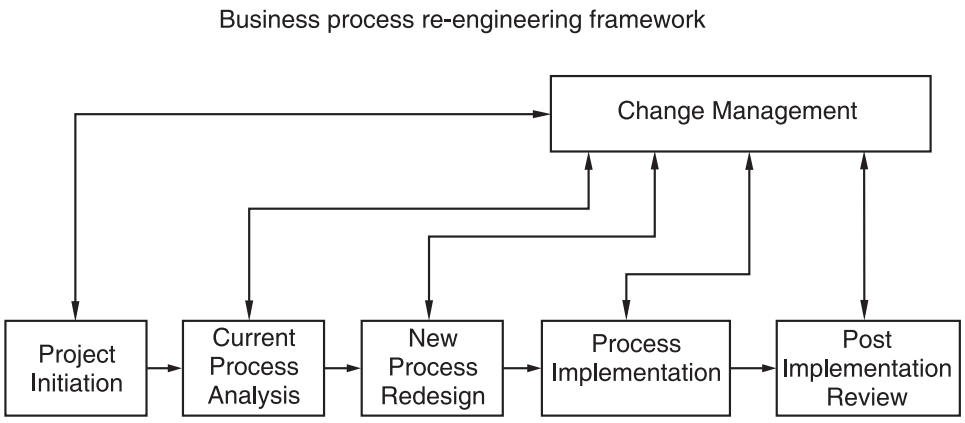


Figure 6.3 Business process re-engineering framework

e-services, and how they would overcome staff resistance to changing to the new process and new system. Each group was given 30 minutes to discuss and prepare their case.

All three groups were able to propose some ways to overcome staff resistance, with their suggestions generalised as follows:

- Secure buy-in from stakeholders through seminars, meetings etc;
- Involve staff members in designing the process;
- Provide training and guidance for affected staff members;
- Ensure transparency and equity in the process;
- Keep communication open and accessible;
- Change measurements to align with the new process;
- Get feedback from staff and respond when needed; and
- Empower staff to make decisions.

In this discussion, Dr Tan was assisted by Devindra Ramnarine and David Spiteri Gingell. Devindra Ramnarine warned the groups that unless the affected staff could realise the benefits to changing to online e-services, most of those affected would not be keen or willing to change. Nobody likes to change unless there is 'something in it for them'. David Spiteri agreed with him and suggested to putting in place a 'change management' programme at the onset of the project.

Dr Tan shared his view on the 'one-third rule': in any BPR project, one third of staff will agree with the change, while another one third will disagree and the remaining one third will be indifferent to the change. The challenge for a change agent is to identify the one third who are indifferent and try to secure their 'buy-in'. Once they are

convinced, it is easier to implement the change with a two-thirds majority agreeing with its going ahead. Tan concluded the discussion by highlighting the importance of the 'business system diamond' for BPR implementation (see below).

Transforming the front office[7]

The 'front office' is the metaphor for those services that deal directly with constituents and clients. During the session on transforming the front office, Dr Tan highlighted the key considerations for such a transformation. They included:

- Value proposition for the transformation – was it for strategic or tactical reasons?
- Legal implications for the transformation – was there the legal framework in place to support online transactions (such as an electronic evidence act, computer misuse act and a data privacy act)?
- Roles and responsibilities of users during the transformation; and
- Prototyping the front office to determine the optimum use of limited resources.

Tan also pointed out the challenge in migrating from hard-copy-filing to e-filing. One would need to determine the cut-off point for e-filing, for conversion of hard copies into scanned files, and archiving of old hard copies. This must be carried out carefully in order to be compliant with the law. According to an EU report, the trend today for front office services is to provide high quality, but relatively simple customised e-government services, based on both Customer Relationship Management (CRM) and data protection principles. Service provision would occur at the appropriate regional or community level, grounded in local situations, responding to the large variety of individual needs of citizens and businesses, and respecting and promoting democracy at all levels.

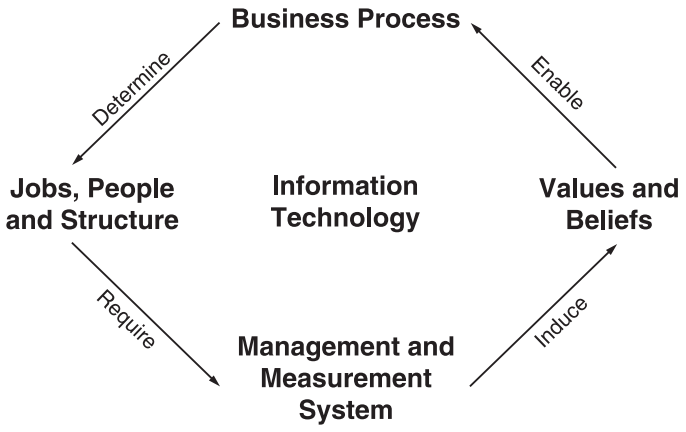


Figure 6.4 Business system diamond for BPR implementation

Enabling the back office[8]

The 'back office' is the metaphor for those services that deal with inter-government and intra-government transactions. For this session on enabling the back office, Dr Tan outlined the trend towards centralisation – even up to national and international levels, exploiting open standards, interoperability, comprehensive security systems, integrated processes and shared databases. Components of the back office include the Web Server, Application Server, Directory Services and Databases. Other considerations for the back office include infrastructure for enabling e-government services, for example, authentication payment and database connection.

The other trend that was noticeable in Singapore was to centralise back office functions – for example, HR, IT, finance and administration functions. This trend would have potential savings due to economies of scale. At the time of the presentation, the Singapore government was in the process of centralising some of these functions for later outsourcing. However, Tan warned participants that this trend might not work in their country for political reasons or because of the influence of unions.

A group exercise on change management[9]

Participants were given the assignment to address the following change management issue: **if more than 60 per cent of the citizens are not interested in using new online e-services, what can be done to change that behaviour?** The three groups were given 30 minutes to discuss and prepare their case. They presented their cases, with most of them having similar recommendations as summarised below:

- Provide a discount for online services
- Provide 24-hour support for online services only
- Conduct a public awareness campaign:
  - Billboards
  - Media talk shows
  - Focus group engagement
  - Jingles and cultural fiestas
  - Set up more kiosks in community centres to reach out to more citizens
- Make online services more user friendly
- Close down all the agency counters
- Make it a law to use online services only
- Educate citizens to use online services

Dr Tan said that these recommendations were useful and that governments could also consider extending the deadline to sign up for online services to boost their usage rate

(based on the Singapore experience). Devindra Ramnarine and David Spiteri Gingell felt that forcing a complete transition to online services was not a feasible option in many countries, given their publics' preference for a range of service delivery modalities.

Infrastructure for e-government[10]

The 'architecture' for e-government refers to the functional arrangement of the various layers of hardware, software and services, which informs the infrastructure for e-government. Dr Tan presented a framework for e-government architecture that was implemented in Singapore, as shown below.

The main components of e-government architecture are as follows:

a. Network layer – This layer looks into the type of networks (e.g. mobile, Internet, virtual private network [VPN] etc.) to enable e-government services. An easy access to the Internet via libraries, post offices and even schools gives members of public – especially the elderly who are often not IT-literate – a convenient and facilitated access to e-government services. Given the digital divide, it is important to pay particular attention to ensuring that every citizen has convenient access to government services online, preferably close to home. It also implies enabling services to be electronically delivered by various electronic media – over the Internet, electronic kiosks, mobile phones, call centres and, in the future, digital TV. The delivery channels for any service should be determined in relation to demand and cost.

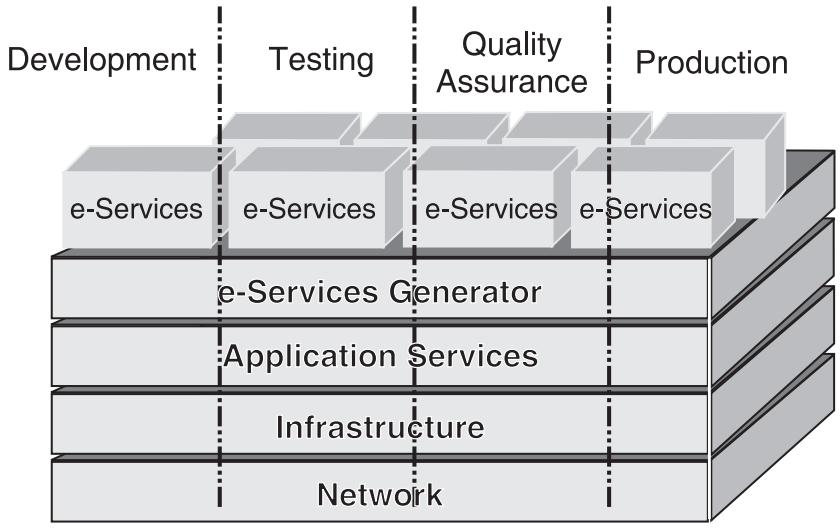


Figure 6.5 Singapore's framework for e-government architecture

b. Infrastructure layer – This layer looks into the basic component of ICT that will enable information sharing. For example, an integrated database system will enable the public service in question to provide an integrated, one-stop service to citizens and businesses, even if processing cuts across several agencies. This will reduce the number of visits to those agencies. For example, the procedure to start a business might involve applying for licenses from various agencies and these being processed sequentially. Any delay in one agency impacts on the service time for applicants. With an integrated database system, some of these processes can be carried out in parallel, resulting in a reduction in service time.

c. Application services layer – This layer provides some of the fundamental application services to support the entire value chain. Examples of such services include payment and authentication services. A flexible e-payment system is recommended to facilitate payment for processing fees and licensing fees, so that applicants are not penalised by having to pay the full fee even if their application is unsuccessful. The charging model needs to be flexible to ensure that applicants are not penalised unfairly in such cases. Another important application service is a public sector authentication system, which gives citizens a secure and convenient way of identifying themselves for the purposes of dealing with government agencies.

d. E-service generator layer – This layer generates e-government online applications by combining the various application services into a complete value chain. For example, the online application for driving licenses requires an authentication service, an e-form for the applicant to complete, an online verification using the integrated database system and finally a payment service to complete the value chain. Each agency can leverage on existing infrastructures and applications to deliver their services online consistently and without having to 're-invent the wheel'. This will reduce the lead-time and investment for rolling out e-government.

e. E-government portal – This is the main portal where all government services are organised into logically-grouped service or functional packages. Some of these logical groupings include employment services, education services, business services and so on. The aim of this portal is to provide a single interface for citizens and businesses to interact with government.

f. Policy and guideline layer – This layer defines essential policies and guidelines that public servants need to comply with during implementation. Examples of such policies or guidelines include privacy policy, public-private partnership (PPP) guidelines and security policies. One of the guidelines that requires special attention is the PPP guideline, which should be in place to guide the public sector when partnering with the private sector in order to play a bigger role in the delivery of online government services. These guidelines need to address fundamental decisions, such as which party (public or private sector) funds the capital and operation costs, as well as who should front the website. Another essential guiding principle is to ensure that commercial interests are not overriding the original intent of government to serve their customers well. Government should avoid competing

with the private sector by following the 'Yellow Page' rule, which states that the government should not be involved in any commercial activity advertised in the Yellow Pages. This also includes advertising on government websites, as well as hyperlinks to commercial websites – which must make clear that they are not public services nor are they endorsed by government agencies.

g. Standards layer – This layer defines standards to ensure consistency and interoperability across different agencies. For example, a standardised monitoring system is needed to measure the success of e-government implementation across all agencies. Deliverables are identified and targets are set for each project to serve as yardsticks to measure e-government progress; these can then be benchmarked against common indicators. Potential benefits to customers (e.g. shorter turnaround time, reduced number of trips etc.) and government agencies (e.g. reduction in manpower, economies of scales etc.) as well as intangible benefits (e.g. a better image of 'one government', improved communication within government agencies etc.) for the country are important criteria for assessing the value of e-government projects. Another consideration is to standardise all agency forms into a single form so that an applicant needs to complete only one application online for various related licences. Other standards include the use of technologies, applications and messages for information interchange.

Dr Tan concluded the session by highlighting the benefits of such an architecture, which would be:

- high availability:
- highly scalable; and
- a secure environment.

The Malta implementation experience[11]

Following the session on system architecture, David Spiteri Gingell outlined Malta's experience in implementing e-government based on the mission: 'To attain a first-class information society that is developing constantly and successfully'. The initial principles and success factors to achieve this objective were set in the year 2000 and are still the mission today:

- Deliver a first-class public service;
- Increase citizen participation in government decision-making; and
- Streamline public services and realise efficiency gains.

In this regard, Mr Gingell (a champion and leader of the e-government programme, formerly of the Ministry for Justice and Local Government and at the time of writing of the Ministry for Investment, Industry and Information Technology) headed an ambitious programme to ensure the timely implementation of these objectives. A number of public and private entities are being included in the initiative to create a unique

synergy that will put Malta on the forefront of e-government in the global ICT scenario.

The Government of Malta has been actively pursuing the attainment of the e-government initiative – treating it as an exciting opportunity that will factually demonstrate to Maltese citizens and businesses the tangible benefits that information and communication technologies can offer to improve their quality of life, streamline public administration and promote improvement in the business community. The initiative has been addressed through a number of inter-linked, parallel implementation streams. Primarily, the government has been actively pursuing public-private relationships with the local ICT sector, looking to establish long-term, trust-based relationships for the design, development and implementation of a range of electronic services. The core operations of the initiative have been developed within government's IT agency, MITTS Ltd, which seeks to provide a common platform and launching pad for all services. The approach, supported by the Central Information Management Unit (CIMU), seeks to achieve a world-class, seamless e-government, including a cost-effective and efficient re-engineering of existing services.

This programme has been an important milestone to the Government of Malta's reform in public administration – initiated in 1987 and still going strong today through the introduction of electronic practices. In this regard, the government has invested heavily in the use of ICT and seeks to invest further in the cultivation of a true information society and economy, a result Malta will benefit from both now and exponentially in the coming years. At the time of writing, a large number of electronic services were being launched across Malta – such as online applications for birth, marriage and death certificates, online submissions of income tax returns and payment of tax, and online applications for examinations. This development and promotion of electronic services is seen as a definite means for meeting citizens' and businesses' expectations and the perceptions of government in a modern world. These efforts towards new channels of communication in an ever more technology-dependant world are Malta's attempts at being more inclusive and receptive to society's needs.

The implementation of the government portal, 'Gov.mt', marked yet another significant milestone. Gov.mt serves as the principal point of entry to all government information and services in Malta. The portal will also change the way the public perceives government – from a 'silo-based' structure to a 'service-cluster' approach, which cuts across the organisational boundaries that exist in the public sector. The introduction of service clusters adds further value, with the presentation of traditional services and their structure being more personal and easy to understand.

Mr Gingell concluded the presentation stating that Malta's government is now planning to put in place a number of essential services – often referred to as 'shared components' – that will service the entire e-government programme, such as a mobile or m-government gateway.

The role of the portal[12]

Dr Tan introduced the role of a government portal and some of the key features that such a portal must include, such as:

- Categorisation of users and their needs;
- Allowing search and index capabilities;
- Managing content from submission to publishing and archiving;
- Providing personalisation to each citizen;
- Integrating with other common applications;
- Enhancing the development cycle using the tools provided;
- Providing software functionality, including redundancy, failover, load balancing and backup; and
- Providing adequate security to ensure the safety of data.

He went on to cite an example from the Land Transport Authority of Singapore (LTA). As the number of its vehicles grew, LTA began to have difficulties coping with the enquiries from the public. To overcome this challenge, LTA decided to develop a portal through which all communication would be interfaced. A strategy was developed using the '5C's': Content, Customer, Commerce, Convenience and Collaboration.

The LTA portal started offering information from the website and extended this to mobile devices. It has since reduced its backlog for enquires and the customer service level has improved dramatically. Dr Tan concluded the session by talking about LTA's successful partnership with a private company to roll out the portal. The partnership involved cost-sharing, revenue-sharing and risk-taking. However, the responsibility for results remains with LTA.

Multi-channel service delivery[13]

Dr Tan went on to present a session on diversifying service delivery. He emphasised the need to 'segment' customers, identifying the appropriate communication channel for each customer segment. For example, customers who are younger are more Internet 'savvy' and more comfortable with mobile services as compared to those who are more elderly. He went on to explain a multiple-channel service delivery, as shown in figure 6.6.

Ideally, a combination of high channel integration (front office) with process integration (back office) will result in offering richer services to customers. This is, in fact, the highest maturity level for e-government. This approach allows customers to access services over different channels and assures that available data are identical in all channels.

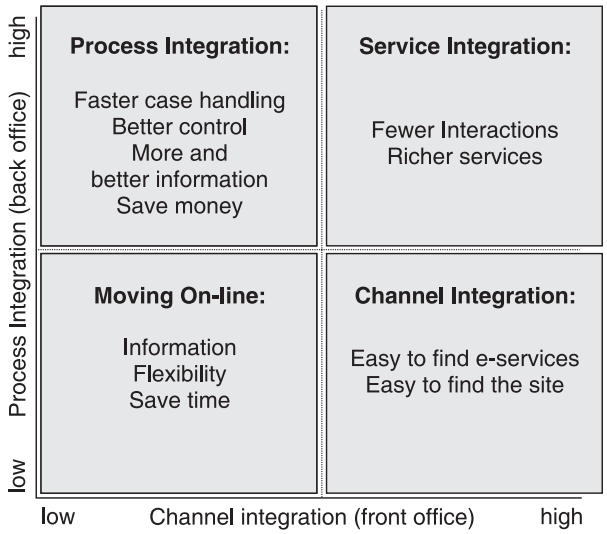


Figure 6.6 Multi-channel service delivery

Group exercise on best practices in e-government service delivery[1]

Dr Tan conducted a group exercise to illustrate best practices. Participants were given one hour to develop a tourism portal to attract and retain tourisms from overseas. They were expected to present their portal design and how it would meet objectives. Participants were divided into two groups: both of the group presentations are summarised below.

Group 1:

- Segment the tourists by country, understand their needs and interests
- Provide the enabling environment in terms of legislation
- Explore PPP to build the portal with a powerful search engine
- Offer special packages and promotion to each customer segment
- Collect feedback from tourists for improvement
- Provide e-payment options

Group 2:

- Gather/analyse available information
- Develop tourism baseline
- Identify niche markets (segmentation)
- Develop portal

- Determine content required
- Determine methods of delivery
- Estimate operation costs
- Identify technology required
- Engage public-private partnerships along the entire development and delivery process
- Provide products and services
- Maintain the portal

Each of the groups did well in applying the concepts learned. Dr Tan continued the session by presenting some of the areas that could compliment their efforts, which included understanding the tourism value chain, as shown below.

There are many stakeholders involved and the portal should cater to all their needs. Thus, the portal should be designed with an end-to-end process – from attracting tourists to retaining them. One method to assist in the portal design is to use the 'mind-map' technique devised by Edward De Bono[15]. The end result of the tourism portal using a mind-map could be developed as shown below.

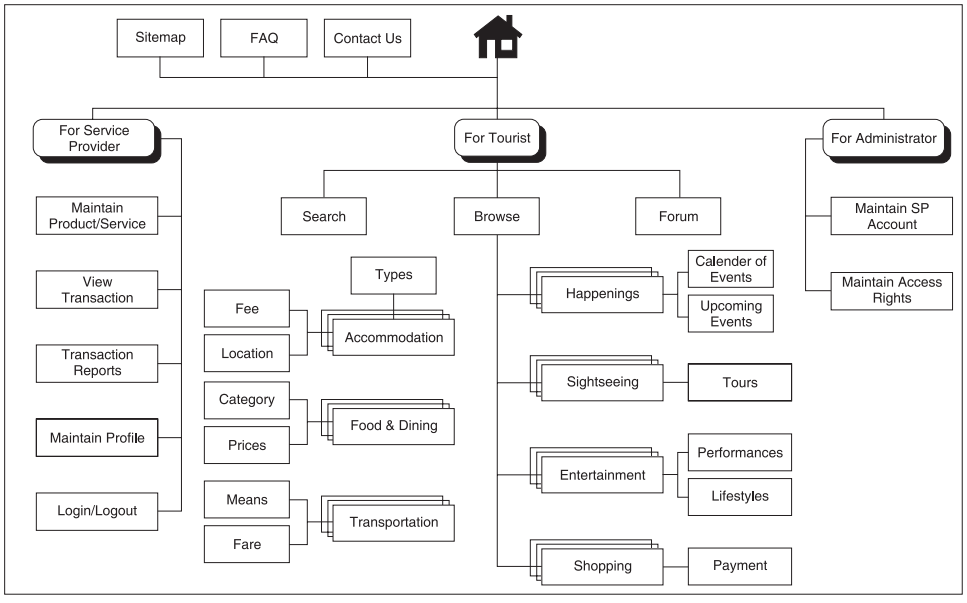


Figure 6.7 A tourism portal designed using the 'mind-map' technique

Site visit to the Civil Service College, Government of Cayman Islands[16]

Participants visited the Civil Service College in UCCI and attended a series of presentations as follows:

a. A welcome speech by Mr Peter Gough on the portfolio of the civil service followed by public sector reform, based on his experiences in several countries. Public sector reform is necessary to drive change when the economy needs to grow, or it might take place due to pressure from donor organisations. Reform can be broad based or by sector, e-government being one of the action plans for administrative reform.

b. An overview of Civil Service College strategies by Dr Hassan Syed, during which he explained why education is becoming lifelong learning, as knowledge learned becomes obsolete overtime. Thus, in order to deliver effective service delivery, public servants need to constantly upgrade their knowledge and be aware of environmental changes taking place due to globalisation.

c. A presentation by Dr Robert Weishan on how to invest in people development for performance improvement. He explained the mission of the college and its key features to provide training for public servants in the Cayman Islands. He updated the participants on college development and partnerships with other institutions to jumpstart course development.

d. A demonstration on 'Angel e-learning' – and how the system can provide busy executives with access to learning after work – was presented by Dr Andy Smith. The course materials for this have been developed by faculty members and used to complement existing classroom lectures.

e. Some of the participants stayed behind to learn more about public sector reform from Mr Gough.

Presentations of work plans and country papers

Selected participants were asked to present their action plans for e-government, either in their organisation or their country.

This concludes the summary of the individual sessions that were presented at the workshop. Chapter 7 goes on to present a comparative analysis of the workshop materials based on criteria developed by The World Bank and by Icfai University, Hyderabad, India.

Notes

1. Commonwealth Secretariat (2007) p. 12.
2. Ibid, p. 13.
3. Shah (ed.) (2005).
4. Commonwealth Secretariat (2007), pp. 12–13.
5. Ibid, p. 13.

6. Ibid, p. 14.
7. Ibid, p. 15.
8. Ibid, p. 15.
9. Ibid, p. 15.
10. Ibid, p. 16.
11. Ibid, p. 18.
12. Ibid, p. 19.
13. Ibid, p. 19.
14. Ibid., p. 20.
15. See http://www.effectivevision.co.uk/EVAHIThinkingTechiques1.pdf [accessed 22 April 2008]
16. Ibid, p. 21.

7

Comparative Plans for e-Government from Small States

The following chapter looks at how the plans for e-government from the participating countries at the Commonwealth Secretariat workshop compare with one another. It also addresses how the prospects for implementing e-government compare to the 'standards' that have been suggested by experts from various international organisations and university business schools.

Comparative analysis of country plans

There were eight country plans (from Barbados, Belize, Cayman Islands, Cyprus, Grenada, Guyana, Mauritius, and Trinidad and Tobago) presented at the workshop.

In terms of **background information** on the history of e-government in the respective countries, a number of themes emerged regarding objectives. These goals were (in no particular order):

- to increase the efficiency of operations;
- to extend ministerial control;
- to reduce costs;
- to centralise accounting procedures;
- to improve the working environment;
- to enhance collegial communications;
- to provide a better service;
- to enable legal and regulatory rationalisation;
- to ensure interoperability;
- to facilitate effective information management;
- to give easier public access to government; and
- to give easier business access to government.

To accomplish these objectives, use was made of: vision statements and mandates; planning committees; new laws and regulations; re-organised departments and branches; additional hardware, software and databases; training of government personnel; various government websites and kiosks; and promotion of these efforts to the public. Not every government had all of these objectives, or used all of these methods, nor did all countries give the same priority to the items they did share – each country assessed its own needs in its own way, and responded with efforts towards e-government that suited their situations.

During the process of building e-government, both past and present, the countries identified a number of **challenges** and **issues**. Given their histories with e-government, and the challenges and issues they face, governments also proposed various **actions**. These, along with e-government background objectives, are summarised in the table below (table 71.). Not all of the actions were proposed by every government, nor did they equally prioritise the actions they did share in common – it all depends on the stage of development, the needs of constituents and the resources available.

Table 7.1 Summarising country plans from the Commonwealth Secretariat Workshop

e-government background: objectives	*Challenges and issues*	*Actions proposed*
• increased efficiency • ministerial control • reduced costs • centralised accounting • improved working environment • collegial communications • better service provision • legal and regulatory rationalisation • interoperability • effective information management • easier public access to government • easier business access to government	• resistance to change • who has rights to and who can access information • incompatibility between technologies • insufficient technology for the purposes proposed • policies and standards • training/skilled personnel • properly licensed equipment • better website design • better service design • organisational co-ordination • predictable budgets	• mobilise support at all levels • provide adequate training • ensure co-ordination • reduce internal conflicts • involve stakeholders • communicate intentions • increase service delivery channels • partner with suppliers • co-operate between gov't departments and branches • expand service offerings • market e-government to ALL users (both within government and in the wider public)

Comparative analysis of e-government prospects: World Bank requirements

Because Dr Albert Tan of Singapore was a major presenter at the Commonwealth Secretariat workshop, and because his materials reflect the World Bank perspective on e-government, it is useful to review the guidelines that the World Bank advocates regarding the building and operation of e-government and e-governance. The World Bank is particularly interested in the integrity of financial transactions and the transparency of government decision-making (because good governance sets the stage for viable commerce)[1] .

In keeping with its focus on commerce, the World Bank emphasises outcomes rather than inputs, throughputs or even outputs. In collaboration with other interested parties, the World Bank has therefore proposed a list of ten requirements for successful electronic governance. The first nine requirements represent the infrastructure that can support the tenth requirement, namely accountability mechanisms (tracking activity electronically so as to provide a 'forensic trail' that can be the basis for assigning responsibility and ensuring accountability).

Table 7.2 World Bank et al's requirements for electronic governance

Vision	Purpose, goals, objectives
Strategic plan	Timetable, resources, personnel
Leadership	Champion, authorisation, publicity
Information sharing	Vertically, horizontally, between project partners
Feedback mechanisms	Contact channels, message recipients, helpful responses
Realistic budgets	Long-term commitment, equipment and training
Cross-government co-operation	Within dept's, between dept's, between govt's
Appropriate technologies	Implement on the basis of availability and cost
Information management	Formatting, storage, retrieval, sharing
Accountability mechanisms	Who is responsible for what, when, where and why?

As can be seen from the table above, The World Bank advocates strategic planning, due diligence, leadership support and adequate funding to make e-governance a success. This is exactly how Singapore managed its transition to e-government, and how it continues to manage its ongoing e-governance. Furthermore the results have placed Singapore at the very top of e-government best practices. However, the Singapore approach is: (a) very costly (no expense was spared to source and use the best electronic infrastructure available); and (b) the mandate and direction was 'top-down' in the planning, implementation and operation. Many other countries do not have the luxury of a large budget or the history of centralisation necessary to support such an approach.

The second part of this chapter considers how the country plans (and more specifically their action proposals) compare with the World Bank's list of requirements (see table below).

Table 7.3 World Bank requirements versus workshop action proposals

World Bank requirements	*Action proposals from country plans*
Vision	Mobilise support at all levels
Strategic plan	Provide adequate training
Leadership	Ensure co-ordination
Information sharing	Reduce internal conflicts
Feedback mechanisms	Involve stakeholders
Realistic budgets	Communicate intentions
Cross-government co-operation	Increase service delivery channels
Appropriate technologies	Partner with suppliers
Information management	Co-operate between gov't departments and branches
Accountability mechanisms	Expand service offerings
	Market e-government to ALL users (in and out of gov't)

There is actually a high degree of overlap, either explicitly or implicitly, between these two lists. The two primary differences appear to be questions of emphasis: in the country plans the 'bottom line' was **a better service to the public** rather than **accountability mechanisms**. Additionally, in the case of the governments involved in the workshop, they did not have the budgets necessary to support all of the elaborate strategic planning of the World Bank approach – therefore planning is likely to be more pragmatic and implementation more ad hoc (as availability of funds and skilled staff permit).

What then will be the kind of impact the extension of e-government and e-governance will have on the countries that participated in the workshop? In another source[2] the World Bank does give an indication of what can be expected from the better public service delivery that e-governance can provide. In their chapter on '**A Simple Measure of Good Governance**', Jeff Hunter, Director of the Office of Debt Management at the U.S. Treasury, and Anwar Shah, a Senior Economist and Project Leader for Public Sector Governance at the World Bank, perform a comparative analysis of the quality of governance amongst 80 countries[3]. What they found were significant statistical relationships between good governance and (a) citizen participation; (b) government orientation; (c) social development; and (d) economic management. In the table that follows the authors consolidate e-governance requirements and the e-governance correlates from the World Bank.

Table 7.4 E-governance requirements and good governance correlates

Requirements	*Correlates*
Vision	Political freedom
Strategic plan	Political stability
Leadership	Judicial efficiency
Information sharing	Bureaucratic efficiency
Feedback mechanisms	Absence of corruption
Realistic budgets	Human Development Index
Cross-government co-operation	Income distribution (inverse of Gini coefficient)
Appropriate technologies	Central bank independence
Information management	Inverse of debt to GDP ratio
Accountability mechanisms	Outward orientation

According to The World Bank findings there is a very clear relationship between good governance and electronic governance on the one hand, and good governance and quality of life (as shown by the above correlations) on the other.

Comparative Analysis of e-Government Prospects: Icfai Business School Guidelines

In 2007, the Icfai University Press of Hyderabad, India, published a book entitled *E-governance in Developing Countries* edited by Santap Sanhari Mishra and Amrita Mukherjee, both of the Icfai Business School Research Centre[4]. The book consists of two sections, one on **Issues and Challenges** the other on **Country Experiences**. It therefore provides a highly appropriate set of guidelines for what to expect from e-governance, which can also be compared to the country plans presented to the Commonwealth Secretariat Workshop.

In their chapter on '**E-Governance in Developed Nations: Lessons for Developing Nations**', Dr Niranjan Pani of the Public Administration Directorate of Distance and Continuing Education at Utkal University, and Santap Sanhari Mishra examine many of the same issues and challenges as dealt with at the workshop. In the section of their chapter on lessons from developed countries the authors are particularly impressed by the example of electronic governance in the United Kingdom. They recommend three characteristics of the UK experience:

- E-governance can be felt even at the local level;
- Development of e-government has been started from below; and
- All e-governance initiatives aim towards satisfying principles of a citizen's charter (the government's accountability to the public).

In this respect, the authors of this chapter, and indeed the authors throughout the book, agree on the priority that the workshop countries gave to **a better service to the public** rather than the World Bank's priority of **accountability mechanisms**.

After reviewing e-governance experience in the US, the UK, Australia and New Zealand, the chapter concludes that **eight factors – four 'Ds' and four 'Ts' – in combination contribute to the success of e-governance**[5]. These factors are listed in the table below.

Table 7.5 Factors for success in e-governance

The 'Ts'	*The 'Ds'*
Transparency	Democratisation
Training	Decentralisation
Technology upgradation	Delegation
Techniques of management	De-bureaucratisation

Once again, these factors seem to concur with the outlook of the participants in the Commonwealth Secretariat workshop. In the section of their chapter on model recommendations for developing nations, Pani and Mishra propose a set of ten principles that can be applied so that they reinforce each other[6].

This time these recommendations concur with both the World Bank and the Commonwealth Secretariat's workshop participants, with the only major difference being the priority of **better service to the public** rather than **accountability mechanisms**. Below, the authors compare all of the proposals mentioned above with respect to e-governance.

Table 7.6 Model recommendations to be applied in a mutually reinforcing manner

Proper infrastructure	Adequate funding
Clarity in policy-making	Benchmarking
Training to manpower	Public-private participation
Management of change	Education
Strong leadership	Attitude reform

Table 7.7 Proposed recommendations and actions for e-government

The World Bank	*Icfai Business School*	*Workshop country plans*
Vision	Proper infrastructure	Mobilise support
Strategic plan	Clarify in policy-making	Provide training
Leadership	Training to manpower	Ensure co-ordination
Information sharing	Management of change	Reduce internal conflicts
Feedback mechanisms	Strong leadership	Involve stakeholders
Realistic budgets	Adequate funding	Communicate intentions
Cross-government co-operation	Benchmarking	Increase service channels
Appropriate technologies	Public-private participation	Partner with suppliers
Information management	Education	Co-operate across government
Accountability mechanisms	Attitude reform	Expand service offerings
		Market e-gov to all users

The World Bank recommendations are broad principles, but they assume 'deep pockets' and 'top-down' control. The recommendations from the Icfai Business School publication are 'theories of the middle range' – wide enough to be generally applicable, yet focused enough to apply particularly to developing nations. The workshop country plans are 'must-do' precepts from practitioners – they must keep the support of both their political masters and public opinion. In each case, each set of recommendations are about what one would expect from each source.

Notes

1. World Bank website, available at: http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTPUBLICSECTORANDGOVERNANCE/0,,menuPK:286310~pagePK:149018~piPK:149093~theSitePK:286305,00.html [accessed 5 February 2008]
2. Shah (ed.) (2005).
3. Ibid, pp. 39–61.
4. Mishra & Mukherjee (eds.) (2007).
5. Ibid, pp. 27–28.
6. Ibid, p. 30.

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).

Appendix I[1]

Article 6

Member States shall provide that personal data must be:
(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
It shall be for the controller to ensure that paragraph 1 is complied with.

Article 7

Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Note

1. European Union Directive on Data Protection, 1995, articles 6 and 7. Available at: http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_8 [accessed 5 February 2008]

References and Bibliography

Agre, Philip E, and Marc Rotenberg (1997) *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press.

Banisar, David (2000) *Privacy and Human Rights 2000: An International Survey of Privacy Laws and Development*. London, UK: Privacy International, and Washington, DC, USA: Electronic Privacy Information Center.

Blood, Rebecca (2002) *The Weblog Handbook: Practical Advice on Creating and Maintaining Your Blog*. Cambridge: Perseus Publishing.

Bounfour, A and L Edvinsson (eds.) (2005) *Intellectual Capital for Communities*. Oxford, UK: Elsevier Butterworth-Heinemann.

Cavoukian, Ann, PhD and Don Tapscott (1995) *Who Knows: Safeguarding your Privacy in a Networked World*. Toronto, Canada: Random House.

Cavoukian, Ann, PhD and Taylor J Hamilton (2002) *Privacy Payoff: How Successful Businesses Build Customer Trust*. Toronto, Canada: McGraw-Hill Ryerson.

Cayman Islands Government, website portal:
http://www.gov.ky/portal/page?_pageid=1142,1595604&_dad=portal&_schema=PORTAL [accessed 4 February 2008]

Commonwealth Secretariat (2007) *Post-Course Report on the Regional Workshop on e-Government Readiness for Effective Public Service Delivery* (4–8 June 2007). Cayman Islands Government.

Davenport, Thomas, and Larry Prusak (2000) *Working Knowledge*. Boston: Harvard Business School Press.

DeLong, David W (2004) *Lost Knowledge*. Oxford, UK: Oxford University Press.

eStrategies Online, EC, *Prompt eGovernment Readiness Can Deliver Huge Savings*, available at:
http://www.britishpublishers.com/ezineezine_120505_EC_prompt_egovernment_readiness_can_deliver_huge_savings.htm [accessed 4 February 2008]

European Commission, *eGovernment Good Practice Framework*, available at: http://www.egov-goodpractice.org [accessed 4 February 2008]

Flor, Nick V (2001) *Web Business Engineering*. New York, US: Addison-Wesley.

Freedman, Alan (2001) *The Computer Glossary, 9th ed.* Toronto, Canada: AMACOM.

Government of Victoria, e-Government Resource Centre, available at:
http://www.egov.vic.gov.au/ [accessed 4 February 2008]

Gurstein, Michael (ed.) (2000) *Community Informatics: Enabling Communities with Information and Communication Technologies*. Hershey, PA: Idea Group Publishing.

Hammer, Michael and James Champy (1993) *Re-engineering the Corporation: A Manifesto for Business Revolution*. London: Nicholas Brealey.

Hiebler, R, T Kelly and C Ketteman (1998) *Best Practices*. New York, US: Simon and Schuster.

Kovai, Zlatko J (2005) *The Impact of National Culture on WorldWide eGovernment Readiness*, available at: http://inform.nu/Articles/Vol8/v8p143-158Kova.pdf [accessed 4 February 2008]

London School of Economics, *DigitalGovernance.org Initiative*, available at: http://216.197.119.113/artman/publish/index1.shtml [accessed 1 February 2008]

Mishra, Santap Sanhari, and Amrita Mukherjee (eds.) (2007) E-governance in Developing Countries. Hyderabad, India: Icfai University Press.

Perri 6 (University of Birmingham) (2004) *e-Governance: Styles of Political Judgment in the Information Age*. Houndmills, UK: Palgrave-Macmillan.

Red de Líderes de Gobierno Electrónico de América Latina y El CaribeRed GEALC: http://www.redgealc.net [accessed 4 February 2008]

Riley, Thomas B and Robert Peter Gillis (1995) *Privacy in the Information Age – A Handbook for Government and Industry Professionals*. Sacramento, CA: Government Technology Press.

Riley, Thomas B (circa 2003) *Security and Privacy: Striking the Balance: A Comparative Analysis of Canada, the United Kingdom and the United States*. Sponsored by Public Works and Government Services Canada, Industry Canada and the Commonwealth Secretariat, London, UK. Available at: http://www.rileyis.com/publications/index.html [accessed 4 February 2008]

Roy, Jeffrey (2006) *e-Government in Canada*. Ottawa: University of Ottawa Press.

School of Computing (Middlesex University) (forthcoming) *Measuring E-Government Readiness in Egypt: Comparative Analysis with the United Kingdom (UK), and Dubai*. See: http://www.middlesex.ac.uk/cs/research/resstudents/na_profile.asp [accessed 6 February 2008]

Schneier, Bruce (1994) Applied Cryptography: Protocols, Algorithms and Source Code in C. New York, US: Wiley.

Seifort, Jeffrey (2003) *A Primer on E-Government*. Washington, DC: World Bank, available at: http://www.fas.org/sgp/crs/RL31057.pdf [accessed 5 February 2008]

Shah, Anwar (ed.) (2005) *Public Services Delivery*. Washington, DC: The World Bank.

Strassmann, Paul (1999) *Information Productivity*. New Cannan, CT: The Information Economics Press.

Turner, Suzanne (2002) *Tools for Success*. London, UK: McGraw-Hill.

University of Manchester's Institute for Development Policy and Management, e-Government for Development, available at: http://www.egov4dev.org/ [accessed 4 February 2008]

Vestel, Wesley (2005) *Mapping Knowledge*. Houston: APQC.

World Bank website, see: http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTPUBLICSECTORANDGOVERNANCE/0,,menuPK:286310~pagePK:149018~piPK:149093~theSitePK:286305,00.html [accessed 8 February 2008]

Electronic infrastructure and network functionality are being utilised by governments around the world. The challenge that developing Commonwealth countries face is that many of them still do not have either the advanced industries or the financial means to modernise governments and their service delivery. This book looks at the obstacles facing developing countries and what lessons they can learn from developed countries' approach towards e-government.

The authors begin by describing the three parallel trends that account for the current circumstances, so that the social, political and technological context of e-government and e-governance in developing countries can be clearly understood. They then review some of the considerations involved for implementing e-governance and e-government. The final chapters give practical examples of working plans for implementing e-government in Barbados, Belize, Cayman Islands, Cyprus, Grenada, Guyana, Mauritius, and Trinidad and Tobago.

Commonwealth Secretariat

ISBN 978-0-85092-878-5