E-Government and Developing Countries: An Overview

SUBHAJIT BASU

ABSTRACT  E-governance is more than just a government website on the Internet. The strategic objective of e-governance is to support and simplify governance for all parties; government, citizens and businesses. The use of ICTs can connect all three parties and support processes and activities. In other words, in e-governance electronic means support and stimulate good governance. Therefore, the objectives of e-governance are similar to the objectives of good governance. Good governance can be seen as an exercise of economic, political, and administrative authority to better manage affairs of a country at all levels. It is not difficult for people in developed countries to imagine a situation in which all interaction with government can be done through one counter 24 hours a day, 7 days a week, without waiting in lines. However to achieve this same level of efficiency and flexibility for developing countries is going to be difficult. The experience in developed countries shows that this is possible if governments are willing to decentralize responsibilities and processes, and if they start to use electronic means. This paper is going to examine the legal and infrastructure issues related to e-governance from the perspective of developing countries. Particularly it will examine how far the developing countries have been successful in providing a legal framework.

Introduction

The aim of this paper is to illuminate the (increasing) evolution, progress and promise of e-government in developing countries and beyond. Beyond in the sense that it will cover the issues, which would be affecting not just the developing countries but also all countries, wherever possible the paper will look into the experience and examples in developed countries and will draw up analogy. The possibilities are exciting: faster access to
government services, lower costs for administrative services, greater public access to budgets and documents and a corresponding increase in the transparency and accountability of government activities. However, with the promise of e-government there would also be the challenges. For instance, the increasing threat of ‘Digital Divide’ causing wider difference between the have and the have-nots. Where the Internet is not available, the technological ‘expertise’ untapped and incentives lacking, the concept of e-government seems highly impractical.

It is not difficult for people in developed countries to imagine a situation in which all interaction with government could be done through one counter 24 hours a day, 7 days a week, without waiting in lines. However, to achieve this same level of efficiency and flexibility for developing countries is going to be far more difficult. Experience in developed countries show that this would be possible if governments are willing to decentralize responsibilities and processes, and if they start to use electronic means. Each citizen could then contact the government through a website where all forms, legislation, news and other information made available. It is assumed that the governments of developing countries, as a collector and source of information, could follow this trend, to serve its customers (citizens and businesses) better and to save costs by making internal operations more efficient, cutting down the complex and over stretched bureaucratic system.

There are many definitions of e-government, and the term itself is not universally used. Definitions of e-government range from ‘the use of information technology to free movement of information to overcome the physical bounds of traditional paper and physical based systems’¹ to ‘the use of technology to enhance the access to and delivery of government services to benefit citizens, business partners and employees’.² The common theme behind these definitions is that e-government involves the automation or computerization of existing paper-based procedures that will prompt new styles of leadership, new ways of debating and deciding strategies, new ways of transacting business, new ways of listening to citizens and communities, and new ways of organizing and delivering information.³ Ultimately, e-government aims to enhance access to and delivery of government services to benefit citizens. More important, it aims to help strengthen government’s drive toward effective governance and increased transparency to better manage a country’s social and economic resources for development. The differences are not just semantic and definitions and terms adopted by individual countries have shifted, as priorities have changed, and as progress has been made towards particular objectives. In the context of the OECD e-Government Project, the term ‘e-government’ is defined as: ‘the use of information and communication technologies and particularly the Internet, as a tool to achieve better government’.⁴

E-governance is more than just a government website on the Internet. The strategic objective of e-governance is to support and simplify governance for all parties; government, citizens and businesses. The use of ICTs can connect all three parties and support processes and activities. In other words, in e-governance electronic means support and stimulate good governance. Therefore, the objectives of e-governance are similar to the objectives of good governance. Good governance can be seen as an exercise of economic, political, and administrative authority to better manage affairs of a country at all levels.⁵

However, as regards to the objective of e-government a distinction should be made between the objectives for internally focused processes (operations) and objectives for externally focused services. The external objective of e-government is to fulfil the public’s needs and expectations satisfactory on the front-office side, by simplifying the interaction
with various online services. The use of ICT in government operations facilitates speedy, transparent, accountable, efficient and effective interaction with the public, citizens, business and other agencies. In the back-office, the internal objective of e-government in government operations is to facilitate a speedy, transparent, accountable, efficient and effective process for performing government administration activities. Significant cost savings (per transaction) in government operations could be the result (Table 1).  

Identifying potential gains from e-government is one thing; actually realising them is another. Implementing ICT projects, particularly large-scale projects that could have a major impact on service quality improvements or efficiencies, could raise a number of problems, many of which relate particularly to operating within government.

### Table 1. Summary of objectives

<table>
<thead>
<tr>
<th>E-government</th>
<th>E-administration</th>
<th>E-governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy coordination and implementation; delivery of services online</td>
<td>Internal and public sector management component</td>
<td>Facilitation of interactions between citizens, government organizations and elected offices including governing and policy-making process</td>
</tr>
<tr>
<td>Developing citizen-centric programs</td>
<td>Strategic planning in transitioning to electronic delivery of services</td>
<td>How technology (particularly the web) is transforming governing process</td>
</tr>
<tr>
<td>Promoting and enhancing citizen participation</td>
<td>Quantifying cost-effectiveness of electronic service delivery</td>
<td>E-federalism: the changing relationship among the levels of government; and E-democracy: enhancing citizen participation online voting, issue of ethic, security and privacy</td>
</tr>
<tr>
<td>Perfecting online service delivery through analysis and evaluation; measuring efficiency and benchmarking against other forms of service delivery</td>
<td>Benchmarking and performance measurement</td>
<td>Legislative and policy-making environment framework; policy initiatives governments are taking: the regulatory framework, implications of initiatives like recognizing the legality of e-signatures, greater citizen participation in policy making environment (e-democracy)</td>
</tr>
<tr>
<td>Country indexing (performance measurement benchmarking) portal analysis, website analysis</td>
<td>Human resource management issues like training and recruitment, deployment of staff and maximizing existing resources</td>
<td>International implications: lowering of borders through information exchanges-impacts and consequences; international standards and best practices; information management and e-government</td>
</tr>
</tbody>
</table>

In order to examine the risk of implementing e-governance solutions the following factors have to be taken into account:

- Political stability (democracy or dictatorial regime)
- Adequate legal framework
- Level of trust in government (perception of service levels)
- The importance of government identity (fragmentation or integration)
- Economic structure (education, agriculture, industry or service)
- Government structure (centralized or decentralized)
- Different levels of maturity (weakest part of the chain determines speed)
- Constituent demand (push or pull)

These external e-government barriers often concern breakdowns, missing components or lack of flexibility in the government wide frameworks that enable e-government. To adapt to the e-environment, governments need to establish a legal framework that treats electronic processes and traditional processes equally.

**Background of E-government**

E-government refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet and mobile computing) that have the ability to transform relations with citizens, businesses and other arms of government. These technologies could serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reductions. Traditionally, the interaction between a citizen or business and a government agency took place in a government office. With emerging information and communication technologies, it is possible to locate service centres closer to the clients. Such centres may consist of an unattended kiosk in the government agency, a service kiosk located close to the client, or the use of a personal computer in the home or office. The e-government is supported by the regulations and policies of e-governance, bringing together IT governance and global governance, as well. This is in turn supported by the digital society developed by the connected environment. However, the society must contend with the effects of the digital divide, which represents those members of the society who cannot or will not access the connecting infrastructure.7

Caldrow wrote in 1999 ‘the term e-government has attained conversational status in just four short years’.8 Therefore, even in the USA, a country that is the pioneer in innovation processes, the term has been circulating for just seven years. On a European level, instead, it was in 1999 that the foundations were laid for ‘Europe 2002, an Information Society for All’ the first action plan of the European Union for the Society of Information,9 which is now being substituted by ‘Europe 2005; an Information Society for All’.10

What does it take to become an ‘e-government’? To start with, the answer is not being simple. The fact is that ‘the quest is multi-dimensional across leadership, policy, economic competitiveness, education, digital citizen services, internal government operations, digital democracy, and enabling technologies for each dimension’.11 Consequently, the first characteristic is according to IBM, the multidimensionality of the e-government process. In order to construct a lasting competitive advantage this multidimensional factor needs to be implemented through the ‘seven e-government leadership milestones’: ‘integration, econ-
omic development, e-democracy, e-communities, intergovernmental, policy environment, next generation Internet. In IBM’s vision, e-government is the foundation framework within which to operate all the different changes in the different sectors, for which it is unthinkable for example to implement e-democracy without e-government. It is now clear how the latter does indeed represent, effectively speaking, 'a change of mind', a total shift in perspective as utilized in the past, a revolution in the way of being of the public administration towards its interlocutors.

Evolution of e-government has some degree of similarities with the evolution of e-commerce. Analogous to e-commerce, which allows businesses to transact with each other more efficiently (B2B) and brings customers closer to businesses (B2C), e-government aims to make the interaction between government and citizens (G2C), government and business enterprises (G2B), and inter-agency relationships (G2G) more friendly, convenient, transparent and inexpensive. Tapscott identified such an evolution sequence for e-commerce. He suggested that organizations matured from initially having a web presence only, to offering transaction services and business front-end and back-end integration (as well as several more sophisticated development levels). E-government also matures along a similar development path, which starts with broadcasting, then interaction, followed by transaction, and finally integration. In broadcasting mode, the government’s presence would be made with static web pages and one-way communication. The format of the early government websites is similar to that of a brochure or leaflet. The value to the public is that government information is publicly accessible; processes are described and become more transparent, which improves democracy and service. Internally (G2G), the government can also disseminate static information with electronic means.

In interaction mode, websites would be able to exchange information or services with citizens, where citizens can enquire, and obtain resources from database backed websites located behind a portal. The interaction between government and the public (G2C and G2B) is stimulated with various applications. People can ask questions via e-mail, use search engines, and download forms and documents. The fact is complete intake of (simple) applications can be done online 24 hours per day. Normally this would only have been possible at a counter during opening hours. Internally (G2G), government organizations use LANs, intranets and e-mail to communicate and exchange data.

At the transaction stage, the public would be able to carry out (financial) transactions with the government. This would require higher levels of processing capability, as well as payment gateways and security implementation. In this situation, complete transactions could be done without going to an office. Examples of online services are filing income tax, filing property tax, extending/renewal of licenses, visa and passports and online voting. Phase three is made complex because of security and personalization issues. E.g. digital electronic signatures will be necessary to enable legal transfer of services. On the business side, the government is starting with e-procurement applications.

Finally, e-governments would reach integration stage where departments collaborate in significant ways to avoid duplication of efforts, and a one-stop contact point is created, which is capable of handling procedures of all involved departments. In this phase when all information systems are integrated and the public can get G2C and G2B services at one (virtual) counter. One single point of contact for all services would be the ultimate goal. The complex aspect in reaching this goal would be mainly on the internal side, e.g. the necessity to drastically change culture, processes and responsibilities within the government institution (G2G). Government employees in different departments have to work together in a smooth and seamless way. In this phase cost savings, efficiency and customer
satisfaction are reaching highest possible levels. Hence, the forces that once converged to promote e-commerce are now driving us to e-government, along with that, the computer literate population in developed countries are increasingly accustomed to self-service. Changes in the population and specifically in the workforce are forcing governments to ‘do more with less’. The trend in the developed countries is to spend a record budget surplus in funding its e-government expenditures.

Because every society has different needs and priorities, there is no one model for e-government and no universal standard for e-government readiness. Each society’s and government’s readiness for e-government would depend upon which objectives and specific sectors it chooses as priorities, as well as the resources available at a given point in time (which might depend on budgets, donors, etc). The necessary pre-conditions for e-government depend upon a society’s most important needs. For example, the level of infrastructure, legal framework and human capital needed for e-government vary with the objectives being pursued. It is also politically intriguing the idea of implementing a generic and adaptable model e-government as it clashes with the understanding that each country and region has its own peculiarities, constitution, and legal and political framework. The idea is also simply unrealistic.

Once a vision and priority sectors for e-government are established, it is important to assess how prepared a society is for e-government. Assessing e-government readiness requires examination of government itself institutional frameworks, human resources (including ICT managers, procurement officers, and others), existing budgetary resources, inter-department communication flows, etc. National infrastructure, economic health, education, information policies, private sector development and other issues are also factors of society’s readiness. Even in developing countries where problems of low connectivity and human resource development (including low ICT literacy) are severe, creativity and careful planning can develop specific applications, services and information that can be delivered in a targeted, useful way to identifiable audiences. A study by Anderson Consulting found vast differences among countries in the maturity of their e-government effort. Perhaps the key finding, however, was that even the most mature countries have tapped less than 20% of the potential (Table 2).

E-government and Developing Countries

One of the success stories of e-government is ‘eEurope’. The eEurope initiatives have been both highly politicized and highly results oriented. The EU has showed its ability to track, monitor and evaluate the implementation of each Action Plan, using a comprehensive system of key indicators and benchmarking reports produced and submitted to leaders for review and further action. The deliberately detailed implementation of eEurope and the political commitment of the EU leaders to construct and actually enforce a knowledge-based economy and society ‘for the benefit of all’, distinguish the EU from other global, regional and sub-regional actors. The positive effects of political will and enforcement through effective implementation benchmarking are perhaps the first lessons that developing countries may well learn from eEurope.

What is more important, ICT or clean water? No country, be it developed or developing, large or small can afford to ignore those gains that ICTs potentially offer. For developing countries this is even more pressing, given the ‘leapfrogging’ opportunities available through modern technologies. I will discuss ‘leapfrogging’ later in this section. ICT and e-governance, coupled with smart and timely government policies, have the potential to
Table 2. Capability index

<table>
<thead>
<tr>
<th>Country</th>
<th>E-government Characteristics</th>
</tr>
</thead>
</table>
| United Kingdom | • Highly Developed E-environment and infrastructure  
|             | • Wide market access and network                                                             |
|             | • European Community standards                                                               |
|             | • Government promoted as exemplar in e-commerce                                             |
| India       | • Emerging E environment and infrastructure                                                 |
|             | • Growing domestic base of world class technical expertise                                   |
|             | • Rapid development of rural E-Commerce through State and local government initiatives       |
| Malaysia    | • Burgeoning E infrastructure                                                               |
|             | • Development of technical expertise                                                          |
|             | • Strong E-government initiatives                                                            |
| South Africa| • Relatively rapid internet progress                                                          |
|             | • Largest African E economy                                                                  |
|             | • Gateway to southern Africa                                                                 |
|             | • Government pushing e-commerce                                                              |
| Singapore   | • Highly developed E environment and infrastructure                                          |
|             | • Gateway to South East Asian markets                                                         |
|             | • Proactive E-Government and E-Commerce related government initiatives                        |


reach development objectives faster and at a lower cost than conventional approaches. One particularly strong opinion questions the very relevance of information society in circumstances of persisting poverty, lack of clean drinking water, widespread corruption, and other characteristics of developing countries that require handling immediately. One cannot deny the vital importance of these and other problems, however it is not possible to avoid that which is unavoidable. The delay in implementation would only cause added cost. However, one can emphasize the importance of regional and sub-regional cooperation in promoting the philosophy of the information society. Table 3 summarizes the impediments to the growth of e-government in developing countries.

Therefore, e-government for developing countries raises some hopes and demonstrates opportunities. Hence, where, do the developing countries stand in respect of the stages of evolution. Before going into the details about the legal implications, it is essential to trace here the required infrastructure of the developing countries in this context. The objective here is to understand the balance of revenue spent to develop such capability and level of utilization. It is beyond any argument that in the context of developing countries, ICT is one of the most significant forces of modernization. Investment in communication infrastructures, and in training and learning, would enable developing countries to increase their competitiveness as external service provider.

A 2001 study of the development of e-Government by UN identified the level of e-government in 190 nations (UN/ASPA, 2001). The study outlined five stages of e-government, spanning from emergence to integration. At the time of the survey, none of the surveyed nations had achieved integration, and only 17 had achieved the transaction stage. Most developing nations were either at the emergence or at the broadcast stage, thus providing very few interactive services to their citizens. Nations with extensive interactive, knowledge supported services typically also maintained a considerable IT and government
Table 3. Factors impeding an enabling e-government environment in developing countries

<table>
<thead>
<tr>
<th>Core Factors</th>
<th>Symptoms</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institutional Weakness</td>
<td>Insufficient planning</td>
<td>Inadequately designed system</td>
</tr>
<tr>
<td></td>
<td>Unclear objectives</td>
<td>Cost over-runs</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Shortage of qualifies personnel</td>
<td>Insufficient support</td>
</tr>
<tr>
<td></td>
<td>Lack of professional training</td>
<td>Isolation from sources of technology</td>
</tr>
<tr>
<td>Funding arrangements</td>
<td>Underestimated project costs</td>
<td>Unfinished projects</td>
</tr>
<tr>
<td></td>
<td>Lack of recurring expenditure</td>
<td>Higher maintenance costs</td>
</tr>
<tr>
<td>Local environment</td>
<td>Lack of vendor representation</td>
<td>Lack of qualified technical support</td>
</tr>
<tr>
<td>Technology and Information changes</td>
<td>Limited hardware/software</td>
<td>System incompatibility</td>
</tr>
<tr>
<td></td>
<td>Inappropriate software</td>
<td>Implementation problems</td>
</tr>
<tr>
<td>Legal inadequacy</td>
<td>Complex legislative procedure</td>
<td>Over-reliance on customer application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lack of legal framework</td>
</tr>
</tbody>
</table>


infrastructure to offer these, and were generally well funded. This raises the question whether e-Government is largely a question of resources, and specifically whether knowledge management requires the provision of considerable financial and IT resources.21

The feasibility of having a successful e-government is directly depended on the governments’ overall ability and readiness to spend on the necessary information technology and related costs. To provide a better understanding of the affordability, Table 4 illustrates IT budgets for some developed and developing economies. Where known, the table also separates targeted e-government funding from overall IT expenditures by the government. Many governments choose not to separate these two and now consider all government IT spending to be e-government spending. The table clearly shows the vast spending differences between developed and developing economies. However, there is another issue to look into. Conventional budgetary structures (such as the one followed by most of the OECD countries: vertical funding structures, in accordance with the core public management principle of holding an agency accountable for achieving organizational objectives and giving it the resources to accomplish those objectives) may not take into account the specific needs of certain most e-government projects, particularly those involving long-term funding requirements and collaboration across agencies. In order to maximize the benefits of e-government for developing countries financing issues must be addressed. One commen-

Table 4. Government IT budgets for developed and developing countries

<table>
<thead>
<tr>
<th>Government</th>
<th>India</th>
<th>Philippines</th>
<th>Hong Kong</th>
<th>USA</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Spending in Million US $</td>
<td>556</td>
<td>120</td>
<td>250</td>
<td>52,000</td>
<td>10,000</td>
</tr>
<tr>
<td>IT Spending as % of Budget</td>
<td>2–3</td>
<td>0.8</td>
<td>1.2</td>
<td>13</td>
<td>2.4</td>
</tr>
<tr>
<td>E-Government spending as Part of IT Budget (%)</td>
<td>34</td>
<td>75</td>
<td>0.08</td>
<td>5.2</td>
<td></td>
</tr>
</tbody>
</table>
Development of e-governments is directly proportional to the IT infrastructure that is capable of supporting and enabling the execution of e-government. An e-government infrastructure in general comprises network infrastructure, security infrastructure, application server environment, data and content management tools, application development tools, hardware and operating systems, and systems management platform. However, many developing countries do not have the infrastructure necessary to deploy e-government services throughout their territory. A recent study by Harris considered that there is a virtually inverse relationship between transitional government budgeting and ICT investments (Table 5).

Development of e-governments is directly proportional to the IT infrastructure that is capable of supporting and enabling the execution of e-government. An e-government infrastructure in general comprises network infrastructure, security infrastructure, application server environment, data and content management tools, application development tools, hardware and operating systems, and systems management platform. However, many developing countries do not have the infrastructure necessary to deploy e-government services throughout their territory. A recent study by Harris compared the ICT situations in six selected developing countries, based on World Bank data for 2000. Table 6 illustrates the availability of two important technologies, telephone lines and personal computer penetration, for several developing countries, as well as the number of Internet users. An interesting finding is that the developing countries are very non-homogeneous with respect to technology availability and use, differing by two orders of magnitude.

In a developing country, the gap between the educated elite and uneducated poor is wide. The educated population have the necessary resources and have the means to use information and communication technologies. There is the possibility that professionals in large cities in China or India may find it about as easy to access computers as their counterparts in the UK or Canada; however the situation would be clearly different for those living in rural areas. This ‘digital divide’ between those who already have access and those who would not gain access for a long time may result in long-lasting and widening economic gaps between the ICT have and have-nots. As a result, the provision of e-government services would be biased, favouring educated, urban residents.

### Table 5. Traditional budgeting and budgeting for ICT investments

<table>
<thead>
<tr>
<th>Focus of traditional government budgeting</th>
<th>Characteristics of high-value ICT investments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-year (or biennial) expenditures</td>
<td>Multi-year investments</td>
</tr>
<tr>
<td>Programme-by-programme performance</td>
<td>Enterprise or cross-boundary performance</td>
</tr>
<tr>
<td>Financial cost/benefits</td>
<td>Financial and non-financial costs/benefits</td>
</tr>
<tr>
<td>Level of effort within existing work flows</td>
<td>Changes in the flow of work</td>
</tr>
<tr>
<td>Ongoing operations</td>
<td>‘Start-up’ operations</td>
</tr>
<tr>
<td>Control</td>
<td>Innovation</td>
</tr>
</tbody>
</table>


### Table 6. Information and communication technology situations in six developing countries

<table>
<thead>
<tr>
<th></th>
<th>India</th>
<th>Bangladesh</th>
<th>Thailand</th>
<th>Malaysia</th>
<th>China</th>
<th>Philippines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed lines and mobile telephones (per 1000 people)</td>
<td>35.5</td>
<td>5.0</td>
<td>142.6</td>
<td>412.3</td>
<td>177.6</td>
<td>124.4</td>
</tr>
<tr>
<td>Personal computers (per 1000 people)</td>
<td>4.5</td>
<td>1.5</td>
<td>24.3</td>
<td>103.1</td>
<td>15.9</td>
<td>19.3</td>
</tr>
<tr>
<td>Internet users</td>
<td>5.0 million</td>
<td>100,000</td>
<td>2.3 million</td>
<td>3.7 million</td>
<td>22.5 million</td>
<td>2.0 million</td>
</tr>
</tbody>
</table>
Table 7. Correlation of Internet access and penetration: cost of access

<table>
<thead>
<tr>
<th>Country</th>
<th>Access cost (% of GDP per capita)</th>
<th>Internet users per 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>16.82</td>
<td>5</td>
</tr>
<tr>
<td>South Africa</td>
<td>5.26</td>
<td>35</td>
</tr>
<tr>
<td>Malaysia</td>
<td>4.85</td>
<td>90</td>
</tr>
<tr>
<td>Singapore</td>
<td>0.84</td>
<td>302</td>
</tr>
<tr>
<td>UK</td>
<td>0.91</td>
<td>554</td>
</tr>
</tbody>
</table>


The potential digital divide is clearly a concern, and yet it applies to many types of public infrastructure, be it roads, airports, or schools. In fact, ICT may offer more hope in this respect than other infrastructures, as technology and communication costs are continuously dropping, and energy for computers can be provided through small power generators or solar cells. As experiences shows, a local village may not have roads, a schoolhouse, or telephone landlines, but with a satellite dish and a cyber cafe, it is possible to be connected to the world. However, connecting people by making investments in the technology would be comparatively an easier job than bringing and keeping them online. The key to encourage citizens in developing countries to use the Internet would be to provide them with compelling content and services that meet their primary needs (Table 7).

Most of the developing countries understand the enormous potential of ICT, not only as a tool for improving governance and creating more jobs, but also more significantly as a means to enhance the standard of living of the people. The ICT policy aims at increased application of IT in all occupations, enhancing the IT industry base, creating a robust state information infrastructure and creating human resources for IT. Although the policy statements of differs from country to country however there are some fundamental similarities in the objectives, which can be summarized as following:

- Upgrading of the standard of living of the people of the state through use of IT in all sectors as a tool to enhance productivity, efficiency and optimum utilization of resources, and through full exploitation of the employment potential of the IT sector.
- Establishment of an information infrastructure comprising a high speed broadband communication backbone, nodes, access network, distributed data warehouses and service locations to cater to the needs of trade, commerce, industry and tourism and also to enhance the delivery of government services to the people.
- Facilitating the flow of direct investments.
- Development of human resources for ICT through increased use of ICT in educational institutions and through academic and training programmers that improve the employability of educated youths in the ICT sector.
- Facilitation of decentralized administration and empowerment of people through the application of ICT.

Currently, there are insufficient numbers of people in developing countries trained in appropriate technologies available to do all the work. Training opportunities are also
straining to meet needs. The digital divide, while closing, demands that multiple-delivery channels be maintained for the near future. Many people are concerned about the issues surrounding privacy and confidentiality, even to the point of opting out of e-government opportunities. Technologically, the lack of a single, unifying infrastructure coupled with differences in implications, applications and data structures increase the difficulty of sharing information between departments and levels. Labour rules and policies particularly in public sector can strongly influence how new tasks and skills are introduced. Geographical boundaries, less important to commerce and communication, are still ingrained in the political process. In some cases, the use of the Internet or other channels has been mandated for government use, whether or not doing so makes sense technologically. Although the expanding economy is providing the funding to fuel the necessary expenditures for e-government, the regulatory framework and funding models are lagging, a situation further complicated by a model in which the groups paying for services are not necessarily the recipients of the services. Finally, although government services are typically seen as environmentally clean, the impact of providing high bandwidth to the curb can be enormous.

However focusing on the achievements of e-governance and ICT for developing countries it would be prudent to mention here some of the success that ICTs presented particularly the opportunities to the disadvantaged to help themselves, seize advantages and demand services or control over their lives that they previously lacked. These examples are multiplying, as collaborative approaches and partnerships between the public and private sectors are demonstrating the broader value of advanced communications services:

- In Brazil’s urban slums, the Committee to Democratise Information Technology (CDI) in four years has created 110 sustainable and self-managed community-based ‘Computer Science and Citizenship Schools’, using recycled technology, volunteer assistance, and very limited funds. CDI schools train more than 25,000 young students per year in ICT skills that give them better opportunities for jobs and education. CDI also provides social education on human rights, non-violence, environmental issues, health, and sexuality.  
- The Association for Progressive Communications and Partner Networks implemented a Gender and Information program. The program gave women in Africa, Asia and Latin America the necessary technical skills, computers, hardware, and networking to plan the UN’s Fourth World Conference on Women and to disseminate the results.  
- An example of how new networking can help sub-national governments to become more responsive and transparent is the case of the state of Andhra Pradesh in India. Andhra Pradesh was the first state in India to design a statewide computerization program covering all levels of the administrative spectrum from the smallest—the Mandal Revenue Offices—to the largest (eSEVA). The state-wide Multi-Purpose Household Survey was launched in 1995 to store large volumes of citizen data and information exchange through networking, and Land registration offices throughout the state are now equipped with computerized counters under the Computer-aided Administration of Registration Department (CARD) project. Before the computerization programme, tedious bureaucracy, and lack of transparency in property valuation resulted in a flourishing business of brokers and middlemen who exploited citizens selling property, since a premium was usually attached to speedy delivery of services.

The success of these projects has reaffirmed the faith in what has been termed as ‘leapfrog’ technology. New, innovative and cutting edge technology could help developing countries
overcome their traditional barriers of lack of telecommunications infrastructures. In developed economies, newer versions of technology are often used to upgrade older versions, but in developing economies where still older versions of technology are often prevalent, the leapfrogging over the successive generations of technology to the most recent version creates more possibility and often provide access to newer, efficient and often cheaper alternatives to traditional capital intensive technologies.\textsuperscript{27}

As the situation stands today it is in the interest of the developed countries to play an important role in promoting technology adoption in developing countries, with international organizations such as UN or the World Bank providing the necessary funds. However, pushing e-government initiatives to achieve a significant impact on establishing a digital society and a connected economy would prove to be an elusive goal without proper investment in basic services such as healthcare, education. E-government solutions and approaches used in developed countries may also prove inadequate without a clear understanding of local constraints and conditions.

\textbf{E-government and Legal Issues}

The success of e-government initiatives and processes are highly dependent on government’s role in ensuring a proper legal framework for their operation. A requirement for e-government processes to be introduced and adopted is their formal legal equivalence and standing with the paper process. OECD governments are aware of the need for framework to provide for enforceable electronic transactions, both in the e-government sphere and for e-commerce, and have taken action. For example, the legal recognition of digital signatures is necessary if they are to be use in e-government for the submission of electronic forms containing sensitive personal or financial information. As of 2003, 26 of 30 OECD countries have passed legislation recognising digital signatures, though a much smaller number have actually introduced applications beyond a pilot phase.\textsuperscript{28}

The key concern for the developing countries would be to identify the legal issues. As explained before in this paper, it would not be difficult to provide definitive guidelines for the developing countries as to what type legal safeguards would be necessary to protect the interests of the government and to create binding and enforceable obligations on the government. However, the developing countries are in different stages or phases of e-government, they differ in their political aspirations and in their structure of government and so their requirements would differ and so would their course of action.

The developing countries would face a few key questions in converting to or adopting electronic processes. To start with, the first question that would arise is the question of legitimacy. Legitimacy may express itself through expressions of authority to act, which is related to but not the same as saying that an action is not illegal. In some settings, the legitimacy of government action would affect the enforceability of the action, either on the part of government against a person subject to that government’s rule or on the part of private citizen against the government. Hence, to provide legitimacy to act electronically can only be conferred by legislative measures and supported by an effective legal framework. This framework should be capable of identifying and addressing legal obstacles to e-government. Legal obstacles may include the differences that exist between traditional data collection requirements (that is, sharing of information collected by and provided to various government agencies) and the ease of electronically collecting and sharing data.

Legitimacy also turns on the standards of appropriateness. What kind of qualities should e-government action have, or some standards it should meet, in order to achieve the desired
level of legitimacy. In certain situations, an electronic process would prove to be ‘good enough’ to meet its legal needs without regard to whether it is comparable to or as good as its prior process. At the other extreme, would be the situation where electronic conversion would require a complete re-engineering of their course of action in order to address the legal risks and issues that a particular system presents or that are not being addressed as effectively in their existing system. Because most of the developing countries owing to lack of resources would still depend largely on their existing paper-based systems as a reference point in their analysis, hence the legal framework would require to have a point of compatibility, which I think would be quite unique for these countries. As the situation stands, at least in the near future most of these developing countries would require having both systems of transactions. In order to achieve the legislative revisions, enactment would be required, as current laws, rules, and regulations might not recognize the legality of electronic documents and processes. For example, legislation should ensure that electronic authorizations, contracts and signatures would have the same legal effect as those done on paper. (However, because of the nature of technology, giving them the same legal effect may change or even eliminate the traditional ways these items are completed, such as the notarising of a document.) Additionally, governments may consider the required quorum at meetings be met through the electronic participation of officials rather than by the officials’ physical presence.

It can be said that much of what a government, or those who deal with a government, would look for in an electronic communication would be a latent degree of assurance as to the security of the communications and their source: who sent them? Any user would primarily be concerned about the integrity of the information communicated, in the sense that it is trustworthy and that it has not been altered since it was sent. Similarly, the concern would also be about jurisdiction. However, the issues relating to jurisdiction would be similar in case of both developed and developing countries. The only point of concern is how it should be addressed. E-government for developing countries would also put the judicial system of these countries to test. Generally, the judiciary in these countries are not always in tune with the use and advancement of technology.

Electronic communications appear particularly susceptible to attacks on privacy; in most of the developing countries, privacy is a softer issue and hence even with proper legal framework it can be argued how far privacy of personal information would be maintained. Likewise, fair access to public services is one element that would bring back the issue of ‘digital divide’ within the developing countries—providing facility to the more able citizens. At some point, this would cause the law to impose constitutional limitations on government’s ability to move wholly online in order to maintain equality.29

The legal status of government documents is always of high importance simply because of the weight of authority. One sees this in the priority they are frequently given in evidence statutes. This could be considered as a higher form of authenticity accorded to these records, but it has an impact on the demands made of electronic communications so that they would deserve the same respect that paper documents receive. Pushing this theme further, it can be argued that the integrity that the public expects of government communications is not just that they are unaltered but their content is true. That is not a question of the medium used.

Finally, government use of electronic communications has to be politically acceptable to the opinion makers of a society. No amount of technical excellence can guarantee that any manifestation of e-government would meet this standard. One does hear from politicians, and sometimes from business people, that government should lead the way to making
people confident about electronic communications being safe and effective. This is a
technical aspect of the legitimacy argument that proper government use can encourage
general use of paperless records,30 but how far the governments in the developing countries
particularly the politicians themselves are comfortable with the technology is matter of
debate.
Not all these concerns are specifically related to developing countries nor do they give
rise to legal consequences, but any discussion about e-government for developing countries
could not be made without discussing these issues. However, the difference would be in the
level of priorities. Some factors would play more important roles in some governments than
in the others.
Ideally, a legal framework that allows for the implementation of e-government processes
and services will:

- Preserve basic public policy goals, such as privacy and security, retention, and public
  access to information.
- Provide the statutory basis of, authority for, and regulations related to the government
  processes and services that may be supplied electronically.
- Assign responsibility for and ownership rights to the data provided and accumulated
  electronically.
- Address the sharing of data collected by one government agency with other govern-
  ment agencies that require the same information.
- Clearly, define jurisdictional responsibilities related to intergovernmental transactions
  and business to government transactions.
- Provide a mechanism by which legal requirements are recognized and enforced.
- Provide a basis for the establishment of fees related to electronic processes and
  services.
- Identify the records that should be maintained, the period of retention and the
  required storage media.
- Not be technology-specific or favour one form of service delivery (traditional or
  electronic).
- Minimize costs and the potential for litigation.

Legislative Approaches
As in every other developed country, the traditionally drawn legislation in developing
countries, drafted largely in a paper-based environment is formulated in a manner not
tailored to the legal recognition of electronically generated, stored and transmitted informa-
tion. This feature of legal systems, is epitomized by the traditional basic requirements
scattered throughout legislation, calling for documents (including, for example, contracts)
to be in ‘writing’, for an ‘original’ to be submitted to various governmental agencies, and
for documents to be ‘signed’ by the purported author. Such traditional formulations can be
found throughout a legislation (e.g. Civil Code, Law of Evidence, Arbitration Law),
affecting diverse activities such as filing of documents regarding movement of cargo
through ports, admissibility in court of computerized banking records, securities trading
and many others. Such paper-based formulations define requirements in public law as to
the form of information that has to be provided to governmental authorities by business
and citizens for various purposes (e.g. applications for permits and licenses, documents
required to be filed with customs, tax and other authorities). Such paper-based notions also
apply to the legal validity of various types of communications exchanged amongst the private sector in its commercial activity. Moreover, this legal condition leaves the evidential value in court of electronically generated, stored or transmitted evidence uncertain at best, or renders electronic evidence inadmissible at worst.

Some of the developing countries have introduced legislation following UNCITRAL Model Law on Electronic Commerce. The advantage, indeed the indispensability of utilizing a legislative approach stems from the fact that it is beyond the contractual power of parties to overcome obstacles such as those described above, to the extent that those obstacles are embodied in mandatory rules of law. Moreover, utilizing legislation to address such fundamental issues provides greater legal certainty than reliance purely on contractual solutions. Hong Kong enacted the Electronic Transactions Ordinance (effective 7 April 2000; enacted 7 January 2000), which covers electronic and digital signatures and electronic records. This act is generally applicable to all communications. South Korea’s Basic Law on Electronic Commerce also covers digital signatures and is generally applicable to all communications. Malaysia has its Digital Signature Bill of 1997, which became effective on 1 October 1998. Singapore’s Electronic Transactions Act of 1998 (enacted 29 June 1998) covers digital and electronic signatures as well as electronic records, and is generally applicable to all communications. Similarly, Thailand’s Electronic Commerce Law 2000 covered electronic signatures and is generally applicable to all communications. In the Philippines, the Electronic Commerce Act of 2000 (enacted 14 June 2000) encompasses electronic signatures, electronic transactions and crimes related to e-commerce. The Electronic Transactions Order of Brunei (enacted November 2000) covers electronic contracts, as well as digital and electronic signatures. India’s Information Technology Act of 2000 (implemented in October 2000) covers digital signatures and electronic records, and is generally applicable to all communications.

Privacy

The right to privacy is fundamental to any democratic society. It is not just ‘a’ regulation but it is recognized as a fundamental right in all major international treaties and agreements on human rights and in the constitutions of most countries in the world, either explicitly or implicitly. The slightest apprehension on the part of a person using the Internet about who will see their personal information and how it will be used would by itself mean that they have lost a basic freedom. Moreover, the more others know about the details of a person’s life, the greater their opportunity to influence, interfere with, or judge the choices the person makes. Having knowledge and control of how personal information is provided, transmitted and used is the key to protecting privacy.

Ensuring that e-government initiatives are in step with society’s expectations in this area is a crucial means of building trust. The challenge facing e-government coordinators and implementers is to respect accepted privacy principles while allowing the benefits of the Internet and other technologies flow to citizens. This balance is of particular importance when considering seamless government services involving data sharing among agencies. Of utmost importance is information privacy, ‘individual’s claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed and used’.

The role of governments regarding privacy protection is twofold and therefore always ambiguous. Governments have to ensure the respect of the rule of law, but do also play a proactive role in the development of a welfare state. Finding a correct
balance between these two roles of the modern State will always remain one of the core problems in the development of a regulatory framework in this area.

Government has a responsibility to provide leadership in developing a culture of privacy protection and security. It should provide this leadership through its roles in the development of public policy, as owner and operator of systems and networks, and as user of such systems and networks. As a user of information systems and networks, government shares a role with businesses; other organizations and individuals for ensuring secure use of the system and network.

The OECD was the first inter-governmental organization to issue guidelines on international policy for protection of privacy in computerized data processing. In 1980, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines) were adopted as a Recommendation of the OECD Council. They were followed by the 1985 Declaration on the Transborder Data Flows, and more recently by the Ministerial Declaration on the Protection of Privacy on Global Networks, adopted by OECD Ministers at the 1998 Ottawa conference, ‘A Borderless World: Realising the Potential of Global Electronic Commerce’. At that conference, OECD Ministers reaffirmed ‘their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data’.

Among the perceived benefits of electronic transactions between citizens and governments is the opportunity to collect ‘customer’ information that can be used as a key input to operational and policy decision-making. It is relevant to point out here one such operation where government uses substantial personal information. It is in the case of billing. Billing transactions are a fruitful source of information that allow strategic planners to sift and analyse transactions to identify key trends and unmet service needs, and, because of this, determine the future operational priorities of an agency. For the private sector, that information is an increasingly significant source of business advantage. The variety and sophistication of online identification technologies have increased accordingly, allowing the ready collection and display of an individual’s personal details, purchasing history and commercial value. In marketing terms, it allows a focus beyond groups and subsets of groups, to the ‘customer of one’. As attractive as this focus might be to public sector planners, the possibility that an electronic transaction will provide an instant window on a citizen’s details represents a real threat to personal privacy while online. If the objective of electronic billing is to encourage citizens to adopt a low-cost transaction channel, the belief that it will permit unwanted intrusions by government agencies into personal information is likely to act as a major disincentive. Technology also further complicated the issue by what is known as ‘Caching’ and ‘Cookies’. ‘Caching’ occurs when any web page accessed by a user is stored by that client’s computer (client caching) or by the network server that provides the user with access to the internet (proxy caching). Caching causes a potential problem where it occurs for profiling purposes. The use of ‘cookies’ is more intrusive, as they have the capacity to build profile on the needs, preferences and patterns of expenditure of any individual visiting particular web sites. Cookies work by placing an identifying code on the hard drives of those who visit the site. This code allows the visitor to be tracked as they travel through the website and to be recognized on subsequent visits.

These technological developments have increased the surveillance potential of the government and prompt the demands for specific rules governing the collection and handling of personal information. The question could no longer be whether information could be obtained, but rather whether it should be obtained and, where it has been
obtained, how it should be used. A fundamental assumption underlying the answer to these questions is that if law allows the collection of personal information, the fairness, integrity and effectiveness of such collection and use should also be protected.

Regrettably, most of the legislation mentioned above does not specifically offer a broad protection of individual privacy. In principle, OECD guidelines specify the following for protection of privacy:

- Personal information must be collected for a lawful purpose;
- Personal information must be collected directly from the individual concerned;
- The individual must be made aware of a number of matters (including that information is being collected, the purpose for which the information is being collected, the intended recipients of the information, and the name and address of the agency collecting the information);
- Personal information must not be collected in an unlawful or unfair manner;
- Personal information must be protected by adequate security systems;
- Individuals are entitled to have access to, and request correction of, personal information held about them;
- Personal information shall not be used unless it is accurate, up to date, complete, relevant and not misleading;
- Agencies must not hold personal information for longer than it is required; and
- Personal information must not be used for any purpose other than that for which it was collected.

However, none of these principles excludes the use of billing transactions to create citizen profiles. They do, however, require that such use is both transparent and done with the consent of the individual concerned. The question for public sector agencies, then, is whether the perceived benefits of this offset the risk that the bulk of citizens will avoid electronic transactions in favour of traditional and therefore less intrusive billing and remittance channels.

Privacy must be addressed in the planning and design of e-government systems since it is much harder to interject privacy protections after a system is built. Government websites and online services should fully comply with the fair information principles outlined. How far the developing countries recognize these issues as legal obstacles is a matter open to argument. Business interests govern policies and practices in most developing countries. Hence governments would find that proposed measures to protect privacy meet the staunch opposition of business interests which see such safeguards as an expense and an unjustified constraint on their right to conduct their business affairs as they wish. Hence, finding a balance between the legitimate need to collect information and the need to protect privacy would become a major challenge for the developing countries.

The developing countries that have developed legislations or are currently developing laws are doing it in an effort to promote e-commerce. These countries recognize that consumers are uneasy with the increased availability of their personal data, particularly with new means of identification and forms of transactions, and therefore that their personal information is being utilized worldwide. Data privacy laws are therefore being introduced, not from a human rights perspective, but rather as part of a package of laws intended to facilitate e-commerce by setting up uniform rules.
Authentication

Authentication is an element of security. Security can be divided into two elements: network security and document security. Security is never absolute; it is relative. The legal implication of an insecure network is caution about what one commits to the network, and how one keeps backup copies of documents. The second element of security is document security, which essentially influences how sure one can be of the answers to three questions: ‘what?’, ‘who?’ and ‘where?’. Document integrity is the first: has the document been altered from what was intended by the parties to a communication? The practical issue for integrity is how one keeps one’s data from being altered inappropriately or from being assed or destroyed by unauthorized persons. Document source is the second element: who made the document and who sent it? This is usually known as the question of authentication. The issue for authentication is how one can be sufficiently sure that one knows who one is dealing with. The challenges faced by the developing countries is not that much different from the developed countries; with only one possible exception that is, developing counties’ governments may be more tolerant of the risk.

How does the government know who it is dealing with? To a lesser extent, how do people dealing with the government know that they are really dealing with the government? There are two elements to this function: identification and verification. There is always a tension between authentication and privacy. As stated before governments have records that can be used to identify people reliability, but privacy laws at least in developed countries limit such activities to known programs and information collected in anticipation of those programs. In practice, much of the discussion of authentication turns on the use of signatures precisely the issue of electronic signatures.

It is not easy to classify the existing legislations with respect to electronic authentication because of the many differences that exist. It is possible, however, to sketch the main approaches at a national and international level. Three approaches can be identified: (1) the digital signature approach; (2) the two-prong approach; and (3) the minimalist approach (Table 8).

The digital signature approach is characterized by its focus on the digital signature technique. Legislation under this category is truly digital signature legislation because it regulates (on the basis of) digital signatures. Legislation under this approach is concerned solely with the (evidentiary) status of the digital signature. The approach has three variants:

1. Technical variant: The technical variant amounts to setting the digital signature technique as a technical standard by means of a legal instrument. The technical variant does not deal with legal consequences, although such consequences may implicitly follow from the use of digital signatures in accordance with the law concerned.
2. Legal variant: The legal variant of the digital signature approach is found in legislation that specifically regulates digital signatures in order to provide this technique with a legal status similar to that of the hand-written signature. The general purpose of these laws is to provide legal security for the use of digital signatures. Often legislation of this kind also includes the implementation and regulation of a Public Key Infrastructure (PKI).
3. Organizational variant: The organizational variant of the digital signature approach neither sets the digital signature as a technical standard nor provides for explicit legal recognition of the digital signature. Instead, it addresses the organization of Certification Authorities (CAs) and the use of digital certificates in connection with
Table 8. Three approaches to electronic authentication

<table>
<thead>
<tr>
<th>Approach</th>
<th>Technology-neutral</th>
<th>Technology-specific</th>
<th>Examples</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital signature approach</td>
<td></td>
<td></td>
<td></td>
<td>Setting digital signatures as technical standard (no explicit legal consequences)</td>
</tr>
<tr>
<td></td>
<td>Technical variant</td>
<td>+</td>
<td>Germany, India</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal variant</td>
<td></td>
<td>Utah, Italy</td>
<td>Legal recognition of digital signatures under certain conditions</td>
</tr>
<tr>
<td>Two prong approach</td>
<td></td>
<td></td>
<td>Japan</td>
<td>Requirements for certification authorities</td>
</tr>
<tr>
<td></td>
<td>Organizational</td>
<td></td>
<td>UNCITRAL (EU, Singapore)</td>
<td>Legal recognition of secure electronic signatures under certain conditions</td>
</tr>
<tr>
<td></td>
<td>variant</td>
<td>+ / -</td>
<td>UNCITRAL (Australia)</td>
<td>Equation of electronic signatures with hand-written signatures</td>
</tr>
</tbody>
</table>


digital signature applications. The aim is to promote trust and reliability in electronic transactions by ensuring that CAs is reliable and secure.37

The second approach is called ‘two-prong’ because of its hybrid way of dealing with electronic authentication. In this approach, legislators aim to make their legislation more time-resistant by addressing certain technological requirements and by leaving room for new technological developments. With this approach, legislation sets requirements for electronic authentication methods that will receive a certain minimum legal status (the minimum prong) and assigns greater legal effect to certain electronic authentication techniques (the maximum prong). The technologies given this higher legal status are referred to as ‘secure electronic signatures’.38

The minimalist approach does not address specific techniques and therefore intends to be technology-neutral. Legislation relates to the functions that signatures may have to fulfil in trade, and the different levels of reliability with respect to the purposes the signatures are used for. Because the main focus of this approach is on the relevant functions of signatures and the ways in which these functions may be translated into technological applications, it is also called the functionalist approach. Within the minimalist approach, the focus on functions of signatures (and writings) can be more or less explicit.39

The market is constantly changing and it is unknown what lies ahead with respect to technological developments. Thus, it might be unwise to issue detailed regulations and to determine specific business models, such as the PKI model, since their viability cannot be ascertained. Viewed in this light, the digital signature approach is seriously flawed. Although, the legislators and regulators subscribing to this approach may do so for all the right reasons (legal certainty, trustworthiness with respect to legal matters), the approach is not recommended as such. The same is true, but to a lesser extent, of the two-prong
approach, which attempts to skirt the uncertainties by presenting an opening for new technologies aside from setting criteria for certain advanced electronic signatures which at present cover digital signatures. The approach is understandable in the sense that there seems to be a strong inclination to look for clear and trustworthy solutions, while at the same time there is a need to leave room for new solutions. Still, within the two-prong approach legislation often deals with issues and situations (e.g. CAs, liability, qualities that focus mainly on certain techniques) that have not yet been determined. Finally, both the digital signature approach and the two-prong approach are in many instances focused too narrowly on signatures as such and not on formal requirements as a whole.

The minimalist approach taken in the UNCITRAL Model Law offers the most sensible solution to legislators wanting to tackle the problem of formal requirements in their legislation. Under this approach, legal requirements of form are generally dealt with in their entirety. Moreover, the minimalist approach allows for different functions which techniques have to fulfil under national legal systems, while creating room for new techniques and adventitious developments. Recent legislative initiatives recognize the advantages of the minimalist approach and have explicitly taken the UNCITRAL Model Law on Electronic Commerce as an example.40

Much of the discussion above put emphasis on differentiating the legal position, which presupposes the presence of paper, and legal position in the electronic age. However, it is interesting to note why one was using paper, is it because it was required by law or is it because of the convenience of paper’s qualities in use. In law, a pencilled ‘X’ may serve as a signature, for example on the will of an illiterate person. However, most people would not accept a cheque with a pencilled ‘X’, in the signature line. What is legal and what is prudent might be different.

The law applicable to e-government is evolving quickly, on a framework of information and technology and public expectations in quick development. The narrow questions of legal authority of government to use electronic communications are relatively easy, particularly as they are now expressly dealt with in enabling statutes based on UN Model Law on Electronic Commerce.41 However, developing countries require specific legislations, which would be capable of accommodating their particular needs. The paper has discussed the main legal question relating to privacy and authentication. It is difficult to legislate with broad application on these subjects, for two reasons: first they to some extent contradict each other, second the technology changes so quickly that laws based on one particular hardware, software or configurations of them are likely to be outdated by the time they are enacted. For developing countries, it is best to be cautious. The law cannot require what technology cannot support. The law for developing countries here is likely to be validating rather than normative. When the gap between a flexible application of current law and demands for new technology grows too great, then legitimacy of e-government comes more severely into question. However different developing countries depending upon their priorities would decide when that point would be and would find a way to act when it arrives.

Conclusion

Hence, what is e-Government for developing countries? A new slogan of the developed world for development of third world or is it a new opportunity of re-organising the instruments and the logic of governing? Probably all of them. However, e-government is an unlikely key for bridging the digital divide. The solution would be to persuade citizens in
developing countries to use the Internet by providing them with convincing content and services that meet their essential needs. Free availability of compelling content may be the single most important action to boost Internet use and reduce the digital divide, but this could clash with protection of intellectual property rights. The best way forward would be to help developing countries in providing the necessary technology. It is going to be the technology that would play a significant role in accelerating developments in area that lags behind on traditional industries. Investments in communication infrastructure and in training and learning would enable developing countries to increase their competitiveness as external service providers. E-marketplaces or national and regional portals could provide new routes for local products, knowledge and skills to be made available on a global basis. Technology can transform governments, making them more transparent and accountable, which would make it impossible to sustain levels of obscurity and corruption that are typical in many of these countries. Last but not least, technology investments in developing countries would boot revenue for vendors that struggle in more mature economies particularly at times when cost-cutting is having a negative impact on new, ambitious ‘e-initiatives’.

Therefore, what is next for developing countries? First, they would require implementing in terms of formulation of national e-strategies according to standards set by internationally agreed principles for information society, and then implementation of the very strategies themselves with modifications according to their own requirements. With only a few exceptions, most of the developing countries are still at varying stages of the formulation/approval process. The delays appear to be a consequence of lack of international cooperation to this end. The implementation phase would require translating commitment into action at both levels: national and regional. The big challenge would be to bring national e-strategies into overall development and governance practices.

Notes and References
2 Deloitte and Touche ‘At the dawn of e-government: the citizen as customer’. Available at www.publicnet.co.uk/publicnet/fe000620.htm.
6 Ibid.
7 Ibid.
9 Presented on 19 and 20 June 2000 at Feira European Council.
11 Caldow, op cit, note 8.


15 The Interact Phase of E-Government: Case Example: Namibian Parliamentary web site—inviting citizens to participate online in their national government. Through its web site, the Parliament of Namibia engages citizens in the democratic process by affording them the opportunity to participate online in political discussions, and the opportunity to stay up-to-date with the legislative developments of the Namibian Parliament. In particular, bills up for consideration are posted online and citizens can send comments directly to parliamentary representatives. The site also links to many regional councils, which have similar web sites. Website: http://www.parliament.gov.na.

16 The Transact Phase of E-Government Case Example: E-Procurement System, Chile—Revamping offline rules and regulations in order to establish an efficient online procurement system. Prior to the establishment of portals to conduct government transactions online, the government procurement system in Chile was fragmented and burdened with various, sometimes contradictory regulatory frameworks. In 1998, the government formed the Communications and Information Technology Unit (UTIC) and conferred on it the mandate of coordinating e-government efforts in an attempt to control costs and bring transparency to the system. The UTIC completely revamped the underlying system of procurement by centralizing all purchasing activities through a central web site. This website automatically sends emails to private companies registered on the system when contracts come up for bid and takes bids online. Not only has the new system streamlined procurement, it has also created new methods of oversight and accountability. For example, the site includes statistics and other information on past performance of government contractors. Website: http://www.compraschile.cl (in Spanish). Case study: http://www1.worldbank.org/publicsector/egov/eprocurement_chile.htm.


26 FRIENDS (Fast, Reliable, Instant, Efficient, Network for Disbursement of Services) is set up in every district head quarters by the IT department. FRIENDS is a unique project taken up by the government to provide the benefits of IT to the common man. This offers the citizen an integrated point for utility payments for specific services such as electricity charges, water charges, property tax, professional tax, building tax, etc. The server of the FRIENDS centre is being linked to the server of the concerned departments for updating on a real time basis. A friendly ‘Help Desk’ helps the customers to fill up forms and clarify their doubts. The project when completed is expected to benefit 12 million people of the state, i.e. about 40% of the population. With a view to disseminate increased application of IT to the rural people, in association with the library council, the IT department has started a novel project called SEVANA. The project envisages converting about 400 libraries in rural areas into IT dissemination centres by providing free Internet connections so that they can function as rural information centres. A software package named SEVANA provides information on various government schemes, programmes, general information on local bodies, links to important sites, and other important facts relevant to the rural population. The pilot project, which was implemented in Kallara Panchayat in Trivandrum district, has been functioning very well. The centre became a point of convergence for villagers seeking information services and an entry into the world of computers and computer literacy. The people from rural areas are able to get various utility services through the Internet. Training for Internet awareness is also being organized in these centres. The Vijaywada Online Information Center (VOICE) delivers municipal services such as building approvals and birth and death certificates. It also handles the collection of property, water and sewerage taxes. The VOICE system uses five kiosks located close to the citizens. These were linked to the back end processes in the municipal offices through a wide area network. The application has reduced corruption, made access to services more convenient, and has improved the finances of the municipal government (known as ‘municipal corporations’ in India. http://www1.worldbank.org/public-sector/egov/voice_cs.htm#top

27 The promise of ‘Leap frog technology’—Navrongo, Ghana, for details visit www.idrc.ca/evaluation/documents/Navrongo/NAVRONO.HTM#information.Wireless Technology in Action—Grameen Telecom (Bangladesh) It is one such success story about a country where teledensity is one of the world’s lowest, an innovative idea based on cutting age technology has been able to by-pass traditional technology, leap-frogging into the information age. See also The Working Group on e-Government in the Developing World ‘Roadmap for e-government in the developing world: 10 questions e-government leaders should ask themselves’ Pacific Council on International Policy, Los Angeles, 2002. Available at http://www.pacificcouncil.org/pdfs/e-gov.paper.f.pdf.

28 OECD, op cit, note 4.


33 OECD, op cit, note 4.
37 Ibid.
38 Ibid.
39 Ibid.
40 Ibid.