A GREEN PAPER ON ELECTRONIC COMMERCE FOR SOUTH AFRICA

EXECUTIVE SUMMARY

TABLE OF CONTENTS

visit
www.ecomm-debate.co.za

OVERVIEW

WHAT IS E-COMMERCE?

E-commerce, broadly, is: "The use of electronic networks to exchange information, products, services and payments for commercial and communication purposes between individuals (consumers) and businesses, between businesses themselves, between individuals themselves, within government or between the public and government and between business and government."

The main benefits are:

- Improved response time.
- Improved competitive positioning.
- Ease of concluding deals and financial transactions.
- Extended global market reach
- Increased revenue potential
- Increased consumer convenience and choice
- Reduced competitive prices.
- Improved and convenient customer service.

Electronic commerce touches all major aspects of economic life and involves integration of elements of technology, laws, infrastructure, business operation and public policy. All elements need to interface as smoothly as possible to yield maximum benefit. It requires new skills and forms of industrial organisation, and must be studied from social and political angles as well as legal perspectives.

UNDERLYING PRINCIPLES FOR THE DEVELOPMENT OF E-COMMERCE POLICY

The development of e-commerce policy in South Africa is based upon the following principles:

- Improving quality of life, using e-commerce to facilitate equitable socio-economic development.
- Ensuring international consistency, alignment and harmony. South Africa needs to be in line with international e-commerce trends and benchmarks while taking cognisance of its own unique requirements.
- Being consultative, transparent and balancing the interests of the broader spectrum of stakeholder by eliciting participation in policy-formulation.
- Being flexible in establishing rules and regulations for governance.
- Ensuring proposed policy remains technology-neutral.
- Supporting private sector-led and technology-based solutions and initiatives.
- Establishing public / private partnerships to promote and encourage the development and use of e-commerce.
- Promoting and supporting small, medium and micro-enterprises (SMMEs) and the informal sector in their speedy adoption of e-commerce.

THE ROLE OF GOVERNMENT

Government will be instrumental in enabling the growth of e-commerce and fostering a stable environment by:

- Providing adequate protective environment and framework.
- Promoting easy and affordable access to information and communications infrastructure as well as technologies.
- Ensuring rapid adoption by SMMEs and the informal sector.
- Promoting and reinforcing education, skills development and awareness.
- Positioning Government as a model user of e-commerce in procurement and service-delivery processes.
- Facilitating the development of a coherent Southern African Development Council (SADC) e-commerce framework.

South Africa's strategic positioning should be viewed in the context of political, social, cultural, economic and technological conditions. The policy framework will:

- Promote business growth and development through innovation and competition.
- Create jobs.
- Expand international trade and create new markets.
- Attract foreign and local investment.

THE GREEN PAPER ON ELECTRONIC COMMERCE FOR SOUTH AFRICA, STRUCTURE AND FORMAT

E-commerce issues and questions raised in the Green Paper are targeted at a wide range of distinct audiences along the following basic categories:

- Persons knowledgeable in the area, such as experts and professionals.
- Individuals and enterprises that use e-commerce.
- Learners in this environment

The Green Paper seeks answers to some of the pressing questions regarding development and implementation of e-commerce policy. It is divided into four main themes:

- Legal and regulatory issues.
- Building trust in the digital economy.
- Enhancing the information communication infrastructure.
- Maximising benefits.

LEGAL AND REGULATORY ISSUES

The legal foundation for e-commerce raises questions and uncertainties concerning the validity, legal effect and enforceability of transactions conducted electronically. Other areas involving legal issues include taxation, customs duties, intellectual property rights, data protection, consumer protection, authentication, and jurisdiction and liability issues.

Legal issues surrounding policy formulation encompass:

- The application of statutory provisions which mandate traditional paper or paper-based concepts such as original, writing and signature to electronic communications.
- Electronic formation and enforceability of contracts.
- Admissibility of electronic evidence.
- Authenticity and integrity of electronic communications.
- Information of material significance to confirm or enforce certain obligations for dispatchers and recipients of goods or services.
- Verification of dispatch.
- Acknowledgement of receipt.
- Management and retention of records.
- Protection of consumers, privacy, security and confidentiality
- Rights of access to information
- New laws applicable and the relevance of the older ones.

Principles underpinning formation of the legal framework revolve around:

- The need for legislation supporting e-commerce transactions.
- The need to ensure transactions can be effected through paper or electronic means.
- The desire to recommend legislation limited to areas likely to increase the overall efficiency of South African commercial transactions. Any proposed legislation should minimise the regulatory burden on business and government, including litigation and costs.
- Ensuring that any laws that adapt the law of contract are technologically neutral.
- Any proposed legislation must conform to existing international standards and rules.

Issues raised in the Green Paper include:

- Types of electronic transactions to be covered by any proposed legislation.
- A uniform commercial code for e-commerce.
- Intellectual property rights.
- Privacy and security.
- Contracting and trade laws.
- Place of jurisdiction in cross-border e-commerce transactions.
- E-commerce and multilateral trading system.
- Electronic payment systems.
- Governance in domain naming.
- Taxation in the e-commerce environment.
- Consumer protection issues.
- Protection of personal data over open networks.
- Institutional and organisational framework.

QUESTIONS FOR POLICY CONSIDERATION

1. Are there areas where South Africa can become a key player in influencing the global e-commerce legal framework?
2. Should the South African legal framework be guided by the model set by UNCITRAL?
3. Which other countries come close to representing a legal framework that will be significantly useful in South Africa's?
4. What laws need to be addressed to shape the South African e-commerce legal framework and how?
5. Does the South African legal system have a rule of law about infringements outside the country's border and other jurisdiction matters? If so, how is judgement enforced?
6. How flexible should be any proposed legislation in ensuring technological neutrality?

CONTRACTING AND TRADE LAWS

The fundamental issues are establishing the validity, acceptability, recognition and enforcement of electronic contracts and communications. South Africa has to determine which of its foundations of contract law are challenged by e-commerce and whether legislative intervention is necessary. Underpinning issues are identified by the UN Commission for International Trade Law Model Law as:

- Ensuring legal recognition for a data message.
- Admissibility and the evidential weight of electronic messages.
- Formation and validity of e-contracts.
- Recognition of electronic documents.
- Time and place of dispatch of electronic communications.
- Offer and acceptance in the electronic environment
- e-Signatures.

Any proposed legislation should provide clarity on how electronic communications will satisfy requirements by law to the extent that:

- An electronic communication constitutes a document.
- Certain information is "in writing".
- Certain information be presented or retained in "original" form.
- Certain documents, records or information be retained.
- A document (electronic communication) is authentic.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent should Government introduce legislation on the legal recognition of electronic documents and communications? What considerations should be taken into account?*
2. *Should legislation prescribe standards to which electronic documents must conform before qualifying as "writing" or "original" and how?*
3. *What exceptions, if any, should be provided for (e.g. wills and sale of land agreements)?*

4. *To what extent should SA refer to international guidelines and national legislative initiatives?*
5. *To what extent should Government introduce legislation on the admissibility and evidential weight of electronic communications, and what considerations should be taken into account?*
6. *Is the current Law Commission initiative sufficient to address the problem? If not, what should the Commission take into account?*
7. *How should the law treat computer evidence generated with and without human intervention?*
8. *To what extent should Government introduce legislation on the formation and validity of contracts and on the recognition by parties of electronic documents, and what considerations should be taken into account?*
9. *Should the law prescribe specific procedures for electronic offers and the acceptance thereof?*
10. *How should the law treat offers and acceptance of offers or other messages expressed as electronic communications generated automatically by computers without human intervention?*
11. *To what extent should Government introduce legislation on attribution of electronic documents and what considerations should be taken into account?*
12. *Should e-commerce be perceived as introducing higher risk?*

SOUTH AFRICAN TAXATION

New technologies such as the Internet have effectively eliminated national borders on the information highway and this poses problems of jurisdiction, enforcement and increased levels of sofistication in terms of conflict of laws. E-commerce further gives rise to an issue concerning the characterisation of income under double taxation agreements: if double taxation treaties are followed, then the question of how taxing rights are allocated must be resolved. There is concern that e-commerce may have the effect of shrinking the tax base and reducing fiscal revenue due to the difficulties inherent in defining jurisdiction in cyberworld, and the problems of administration and enforcement. Areas of immediate concern to the SA Revenue Service, which could have a serious impact upon the effectiveness of ensuring tax compliance in respect of e-commerce, are:

- Residence Basis of Taxation. With effect from tax years ending on or after 1 January 2001, South African residents will be taxed on "worldwide" income, irrespective of where income was earned.
- Electronic Money. Principles governing access to the records of electronic money-issuers need to be established.
- Identification of Website owner. The following information should be furnished on any commercial Website owned by a South African resident, company, close corporation or trust:
  - trading name of the business;
  - physical as well as postal address;
  - e-mail address, telephone or other contact information;
  - statutory registration number in respect of companies, close corporations and trusts.

Many commentators are of the opinion that there is no need at this stage for the implementation of any new taxes relating specifically to e-commerce and that, with modifications where necessary, existing legislation is capable of coping with risks relating to e-commerce transactions.

QUESTIONS FOR POLICY CONSIDERATION

1. *What further challenges does e-commerce pose on taxation?*
2. *What further measures and mechanisms should be put in place to address the challenges?*
3. *What implications does Internet gambling have on fiscal revenue and foreign exchange control policy?*
4. *How should indirect taxes on electronic products be collected from consumers?*
5. *What implications does electronic money have on foreign exchange control policy?*
6. *What principles should be established to give access to the records of electronic money?*
7. *SARS has already indicated some perspectives in the tax administration of electronic transactions. What other views and proposals should be taken into consideration?*
8. *Is there any need to introduce new taxes on electronic commerce transmissions? If so, how should they be administered?*
9. *Should there be specific tax incentives introduced to encourage the development of e-commerce?*

THE MULTILATERAL TRADING SYSTEM

There is an agreement among Governments that the international and domestic regulation of commerce has been, and will continue to be, dealt with in various international forums. The World Trade Organisation stresses that the various forms of electronic transaction comply with its rules and regulations and South Africa, as member, must take cognisance of its WTO commitments in formulating its domestic e-commerce policy. The Multilateral Trading System (MTS) is embodied in the WTO, which comprises 136 member nations and is the only international body dealing with the rules of trade between nations. In dealing with an e-commerce MTS, the concerns that should be addressed are market access for products conducive to e-commerce; issues linked to customs valuation, import licensing, rules of origin, technical barriers to trade and tariff concessions; and classification of e-commerce transactions, for example, trade in goods and services.
At the second WTO Ministerial Conference in Geneva in 1998, Ministers declared:

- The General Council would establish a comprehensive work programme to examine all trade-related issues relating to global e-commerce, taking into account the economic, financial and development needs of developing countries, and to report on the progress of the work programme.
- Member countries would continue to refrain from imposing customs duties on all electronic transmissions (referred to as the "moratorium"). The failure of the later Seattle WTO Ministerial Conference to reach consensus on trade negotiations has hampered development of the MTS, causing confusion and ambiguity on the status of the moratorium.

The Trade and Development Committee has been primarily concerned with the potential of e-commerce to promote economic growth and development in developing countries. Developing countries can play a vital role in promoting the growth of e-commerce within and among themselves by instituting appropriate educational, industrial, technological and economic policies. Developed countries and multilateral organisations should provide technical assistance and human development programmes to enable developing countries to make the transition from "traditional" to "information" societies. Anything less will result in a widening gap between rich and poor countries.

E-commerce should not be viewed solely as a sector of economic activity but as an instrument that can aid developing countries against economic marginalisation. A key challenge is the development of programmes to leverage foreign investment into local telecommunications.

QUESTIONS FOR POLICY CONSIDERATION

1. *What is the impact of the moratorium on levying duties on electronic transmissions in South African and SACU customs revenues?*
2. *What approach should SA adopt in positioning the country and other developing countries in the debate within the WTO, and how should the views of business, labour, NGOs and civil society be articulated?*
3. *Is there a need of domestic regulation of e-commerce?*
4. *The fact that many services can be delivered electronically has implications for most countries' services-provision commitments, since many of these commitments were made without consideration of electronic delivery. What is the potential impact of this on SA's commitments?*
5. *What are the potential consequences of SA's services-provision commitments if e-commerce is classified as either mode 1 (cross border supply) or mode 2 (consumption abroad)?*
6. *How can SA, as chair of the Non-Aligned Movement and member of other multilateral and regional organisations use its influence to advance technological development?*
7. *What role can SA play in promoting the growth of e-commerce in SADC and the rest of Africa?*

INTELLECTUAL PROPERTY RIGHTS

The issue of copyright, trademark and patent protection in an electronic environment constitutes a serious challenge to the development of e-commerce as new technologies challenge existing legislation and enforcement mechanisms.

Intellectual property rights are legal means to protect and balance the interests of an individual against those of the public in terms of disclosure, dissemination, alteration, use and abuse of ideas, with an exclusive right to control and profit from invention and / or authorship of such intangible goods, services and ideas. The World Intellectual Property Organisation (WIPO) classifies intellectual property into two categories; industrial property (such as inventions, trademarks and industrial designs) and appellations of origin and copyright literature (items such as musical, artistic, photographic and audio-visual works).

Some of the problems around the adaptation, protection and enforcement of intellectual property rights in e-commerce are:

- Excessive regulations limiting or discouraging generation, use and sharing of ideas.
- Difficulty in distinguishing between the original owner and the host or custodian of intellectual property in an electronic environment.
- Availability of inexpensive (sometimes free) sophisticated and innovative methods for reproduction and distribution.
- Absence of adequate legislation relating to the protection of South African intellectual property.
- Limited capacity, instruments and mechanisms to monitor and protect intellectual property rights.
- Ever-changing technological innovations relating to the use of the Internet for commercial transactions.
- Dominance of developed countries in creating intellectual property.
- The global nature of e-commerce as opposed to the traditionally local or territorial nature of intellectual property laws.
- An inadequate legal framework to regulate rights and responsibilities for and on behalf of Internet Service Providers in terms of liability.

South African intellectual property law is not fully equipped to deal with the implications of the Internet, convergence, multimedia, digital technology and e-commerce. The application of traditional copyright law to open, public, global networks is hampered by the fact that protection of intellectual property rights has always specifically referred to the protection of information contained in tangible media such as books. Violation of copyrights is difficult to monitor in the electronic environment, since content is not tangible and can be distributed without being copied.

QUESTIONS FOR POLICY CONSIDERATION

1. *How should liability be determined in copyright infringements given intangibility and documents in transit?*
2. *What is the potential liability of end-users "reproducing" infringing copies (transient copies) of copyrighted works by the mere act of viewing them on their PC's, etc?*
3. *How do we strike a balance between enforcing and monitoring intellectual property rights, and promoting e-commerce and cyberspace publishing?*
4. *Is framing (the incorporation of a Website within a Website) and hyperlinking (the creation of digital paths linking two or more Websites) an infringement of copyright?*
5. *What constitutes fair use of copyright material in an electronic environment?*
6. *Who should hold the rights of a trademark registered in different jurisdictions by different parties almost at the same time? What is the basis of determining this?*
7. *Do there appear to be shortcomings in terms of the Trade Marks Act of 1993 in terms of addressing the digital or electronic environment? If yes, what are those shortcomings and what amendments need to be implemented?*
8. *Should there be a linkage of administration between trademark registry and domain name registry to prevent cybersquatting?*
9. *How can SA utilise digital technology to promote protection of indigenous knowledge?*
10. *What are the implications of existing treaties in terms of SA's capacity for monitoring and enforcing violations of intellectual property rights protected by these treaties?*

11. *What proposals can SA make in the upcoming Agreement on Trade-Related Aspects of Intellectual Property (TRIPS) review to ensure the development dimension is entrenched?*
12. *Does South Africa's intellectual property law address challenges posed by e-commerce?*

BUILDING TRUST IN THE ELECTRONIC ECONOMY

One of the main differences between e-commerce and traditional commerce is that electronic transactions are largely impersonal and anonymous. Internet privacy and security fears must be addressed since they deter the adoption and use of e-commerce. Legal, procedural and technical means to ensure security and protect privacy must provide a balance between the ability to combat online criminal activities and providing opportunities for users to exploit new technologies.

Transmission of information over the Internet for trading and communication purposes presents new and sophisticated threats for both the senders and recipients of information. To ensure online transaction security, the following elements are necessary;

- Authentication securing the identities of the parties to a transaction.
- Confidentiality ensuring information is kept private.
- Integrity ensuring the information or process has not been modified or corrupted.
- Non-repudiation ensuring neither party can refute that the transaction occurred (i.e. the transaction is binding).

Apublic key infrastructure (PKI) makes it possible for one Internet user to identify and trust another user (another person, a computer, hand-held devices and / or another electronic entity). In a PKI, digital identification (called a digital certificate) is used to prove the identity of a user or verify a digital signature created by public key cryptography. The goal of a PKI is to establish and maintain a trustworthy networking environment by providing keys and certificate management services that enable cross-application encryption and signature capabilities. Digital signatures are one of the primary ways public key cryptography can be used to make Internet communication safer.

While cryptography has many benefits, the same technologies can be used to hide trans-border criminal activities and threaten national security. A Certification Authority (CA) is a trusted third party responsible for creating, distributing, and revoking digital certificates. These authorities can be commercial and / or governmental.

QUESTIONS FOR POLICY CONSIDERATION

1. *To what extent do existing laws have an impact on the development, use and sale of cryptographic materials?*
2. *Should South Africa adopt specific policies and legislation to encourage and / or restrict the use of encryption in commercial data transmissions or should it take its cue from what is being formulated by other countries?*

3. *To encourage greater public confidence, should Government endorse certain cryptographic methods or CA institutions?*
4. *What restrictions, if any, should be placed on the use and sophistication of cryptography in domestic businesses' electronic transactions?*
5. *Should law enforcement agencies have access to public keys to private cryptographic technology? What rules should apply and which institutions should be involved?*
6. *How should South Africa participate in international deliberations and agreements toward common standards for cross-border data security and access? Should South Africa have its own local / proprietary standards?*
7. *To what extent should the State be involved in the control and interoperability of encrypted material?*
8. *Should there be control of the production, sale (both export and import) and use of encrypted material?*
9. *Should South Africa adopt the Organisation of Economic Co-operation and Development's guideline as benchmark?*
10. *Are there unique circumstances that will need special mention or a different set of guidelines from those of the OECD?*
11. *Where CAs are to be licensed, will it be necessary to define general policies or guidelines and appoint an official agency to issue licenses and monitor compliance with policy standards?*
12. *What should be the general policies or guidelines governing CAs?*
13. *What architecture should a South African PKI / CA have?*
14. *Should legislation be passed to require mandatory or voluntary licensing of industry CAs, and what structure should the licensing regime take?*
15. *Which agencies should be responsible for establishing policy and for managing and implementing the licensing?*
16. *What should be the obligations and responsibilities, and potential liability, of publicly licensed CAs with regard to electronic transactions, electronic signatures, and cryptography?*
17. *Should UN and EU standards apply to the makeup and operations of licensed CAs?*
18. *What organisations can be licensed to be CAs? Will unlicensed CAs be allowed to offer services?*
19. *To what extent should policy draw on and be reconciled with emerging international standards for certification and the potential for competing CAs and certification procedures, applying to transactions across international boundaries?*

LEGAL ISSUES PERTAINING TO PRIVACY

Public safety, crime control, national intelligence agencies and regulatory requirements all require accurate information and evidence about activities of criminal elements. The effectiveness of these agencies in monitoring criminal activities, investigating and prosecuting offenders often depends on their ability to conduct electronic surveillance of communications and to search or inspect places (including computers) for relevant information. There is, however, a concern that key recovery or weak encryption gives Government too great a technical capability to engage in mass surveillance. While there are legitimate reasons for providing lawful State access to encrypted information, implementation raises human rights concerns.

CONSUMER PROTECTION

Government must investigate and identify possible mechanisms for protecting consumers against dangers resulting from the ease and convenience of buying online. Consumer confidence also requires that consumers have access to fair and effective redresses if they are not satisfied with aspects of the transaction. To ensure strong and effective consumer protection in an online environment, alternative and easy-to-use mechanisms for dispute resolution, redress and enforcement mechanisms are required.The electronic market gives established marketers and new entrepreneurs low-cost access to a virtually unlimited customer base. With these benefits comes the challenge of ensuring the virtual marketplace is a secure one to purchase goods and services, and access information. Consumers must be confident that goods and services offered online are fairly represented and that the merchants with whom they are dealing (many of whom may be located in another part of the world), will deliver goods in a timely manner and are not engaged in illegal practices.

Consumers must furthermore be protected against unsolicited goods and communication; illegal or harmful goods, services and content; insufficient information about goods or their suppliers; the accessibility of Websites; invasion of privacy; lack of protection through unfamiliar, inadequate or conflicting laws of a foreign country being applicable to the contract; and cyberfraud. Suppliers are in danger too, being exposed to unknown liabilities especially in view of the fact that Internet commerce law is as yet poorly defined, and differs from country to country.

In line with international standards, South Africa should consider developing adequate measures for consumer protection that include:

- A review of consumer rights legislation and, where necessary, the widening of relevant definitions.
- The creation of industry codes of practice.
- The institution of "Seal of Approval" programs.
- Collaboration between industry and Government in educating consumers on their rights and the meaning of "Seals of Approval".

Only if these measures fail should additional legislation be considered.
At the same time, e-communications and e-commerce must provide new opportunities for small, medium and micro enterprises. Government should recognise the vulnerabilities of inexperienced entrepreneurs, making them aware of their opportunities, responsibilities and liabilities. Responsibilities include checking and confirming incoming e-mail; confirming orders; checking links to and from their Websites, maintaining control over their own content as well as that of sites to which they are linked and if necessary disclaiming links.

Privacy, or the lack thereof, in e-commerce is a major concern and includes not only the privacy of communication between parties in a transaction (e.g. the protection of credit and debit card numbers) but also the accumulation of personal data at Websites visited. The Organisation for Economic Co-operation and Development (OECD) has established guidelines on the protection of privacy and trans-border flows of personal data.

QUESTIONS FOR POLICY CONSIDERATION

1. *How should South Africa embrace international principles in its consumer protection laws?*
2. *To what extent should laws regulate consumer protection, and to what extent can commerce be trusted to regulate itself?*
3. *What new or amended consumer laws and regulations need to be established or adopted in the context of e-commerce?*
4. *Should new bodies be established, particularly to generate awareness?*
5. *How should existing bodies be enhanced to deal with consumer issues and e-commerce?*
6. *Given the ease of access and problems associated with lack of protection from information, what would be appropriate for South Africa?*
7. *What policies need to be put in place regarding administration of private information collected online?*
8. *Should privacy legislation be enacted and, if so, to what extent should the OECD guidelines be taken into account?*
9. *How should the issue of liability for the perpetration of illegal activities via the Internet be addressed, including the roles and accountabilities of ISPs, merchants, banks, Web-hosting and design services, and end-users?*
10. *Should consumer protection and law enforcement issues form part of the subject matter of this Green Paper, or should their respective ministries and Government departments address them from time to time?*
11. *Should South African laws be established independently, or should the initiative come from international treaties?*

ENHANCING THE INFORMATION COMMUNICATION INFRASTRUCTURE

The growth of e-commerce depends on broad and affordable infrastructural access enabled by the convergence of technologies, visionary telecommunications policy, robust network infrastructure, sufficient bandwidth and support for targeted applications. The infrastructure foreseen for e-commerce in South Africa will have to be capable of handling many services and applications, while the availability of (and access to) broadband infrastructures will be crucial for establishing innovative e-commerce services.

The information communications infrastructure upon which e-commerce is based comprises transmission network, hardware and software components. The advancement and integration of the essential infrastructures upon which these technology components rely has fuelled e-commerce growth world-wide. However, the comparative lack of such infrastructure throughout many parts of the developing world severely prevents e-commerce from flourishing there.

The challenge confronting South Africa is creating an ideal e-commerce market structure that will stimulate and modernise network development and infrastructure, accelerate universal access, support affordable access, and encourage investment and innovation. Because of the critical nature of these issues, Government and the business community are faced with the challenge of developing strategies and policies that will strengthen the infrastructure needed to support effective e-commerce.

QUESTIONS FOR POLICY CONSIDERATION

1. *How can regulation promote development of infrastructure components?*
2. *What incentives and obligations should be put in place to encourage investment in new carrier networks and services, in a manner both commercially viable and socially beneficial?*
3. *What competitive and legal environment will be most effective in creating and encouraging new investment in transmission networks, innovation, and network-evolution so customers have a choice of service (e.g. broadband multimedia, multi-service converged wireline, wireless satellite, fixed and mobile capacity)?*
4. *Wireless broadband has great potential for e-commerce so it is important to study spectrum allocation mechanisms. What mechanisms can be used to allocate spectrum without increasing access costs?*
5. *Are user-access bandwidth requirements likely to outstrip network capability? What mechanisms should be utilised in broadband access technology to ensure user's access bandwidth requirements do not outstrip network capability?*
6. *What policies could facilitate and help reduce the price of access?*
7. *What can be done to accelerate Internet access for the rest of the population? What technical and financial means should be employed to promote ISP services in rural areas?*
8. *What kind of partnership should be developed between the private and public sectors to assist SMMEs and communities to access the Internet and adopt e-commerce?*
9. *How do we ensure access (including appropriate facilities) for disabled people?*
10. *In some countries, pricing for local loop access is regarded as the key to e-commerce. Is the unbundling of local loop (local end of transmission networks) likely to play an important role in addressing affordability problems in South Africa? If so, what mechanisms should be used to ensure speedy unbundling?*
11. *Is the existing telecommunications regulatory framework adequate to deal with e-commerce?*
12. *How could the regulator's role be enhanced?*
13. *What should be the priorities and objectives for telecommunications market development and how will they be achieved?*
14. *What incentives and conditions could attract new entrants, particularly small operators in the context of black economic empowerment?*
15. *Certain licensing requirements are seen to have a tendency to prevent innovation, competition and hence limit efficient operation. Should existing licensing conditions and requirements be reviewed, given the advent of convergence?*
16. *Should telecommunications companies provide broadcasting services and vice versa?*
17. *Should regulation in terms of ownership of broadcast facilities continue?*
18. *What are the implications of convergence and e-commerce on competition policy?*
19. *Should the market place determine technical standards and other mechanisms for interoperability?*

DOMAIN NAMING

Domain names are Internet addresses allocated to users on application to institutions assigned with the responsibility of allocating addresses locally and worldwide. A system associating names with each user, referred to as a Domain Name System (DNS), was established to enable users to locate computers and other devices easily. Domain names are also significant business identifiers and, as such, come into conflict with the system of pre-Internet identifiers protected by intellectual property rights. In developing policy, South Africa's overall governance goal should be to enhance the welfare of all those who operate and use the Internet as well as extending it to an under-population of users. Issues of concern regarding the registration and management of domain names revolve around:

- Dispute resolution: trademarks vs domain names. Registrars of domain names are not required to verify whether names that are to be registered are protected through trademarks. This has led to abuse by people who see potential profit through registering a domain name and selling it to any company that might want to use it.
- Potential security concerns. It is important that all registrars of the DNS be competent and able to administer the system correctly. This would include developing regular security-software upgrades for servers.

CURRENT SITUATION IN SOUTH AFRICA

A new governance structure for domain names in South Africa is required. In addition to other submissions in this regard, the Department of Communications has proposed that an independent Domain Name Authority (DNA) be established. This non-profit organisation will represent stakeholders within the information communication technology (ICT) industry, the private and public sectors, and the general public. The DNA would, among other things, look at issues such as provision of universal Internet addresses and deal with the question of dispute resolution and trademark "cybersquatting". The body will acquire accreditation from an international organisation such as the US-based Internet Corporation for Assigned Names and Numbers (ICANN).

QUESTIONS FOR POLICY CONSIDERATION

1. *What should be South Africa's position regarding international processes and structures effecting Internet governance?*
2. *What should be the role of the private sector and Government in managing domain names?*
3. *Is the proposed framework to administer domain naming adequate? How should it be financed?*
4. *What criteria should be applied for the business, technical environment and processes of registration so DNS stability is maintained?*
5. *What suggestions do potential users (notably SMMEs) have on how domain names might be managed?*
6. *What would be the barriers of entering the market at the registry level?*
7. *How should we promote access to Internet addresses?*

ELECTRONIC PAYMENT SYSTEMS

Payment systems in the e-commerce environment refer to methods or instruments of effecting payment through electronic means. E-commerce payments rely on the intermediary role of banks, credit card companies and other financial institutions. Challenges relate particularly to emerging payment mechanisms which can either be network-based or stored-value ("smart") cards some of which have the potential to exchange value (payment) without direct linking to bank accounts.

Even if these mechanisms can be made secure and effective from the consumer's perspective, they may not always be the most efficient ways of transferring funds over the Internet. Other alternatives include "digital cash" (also referred to as "electronic money") and prepaid accounts. Some of these might serve customers who lack access to full banking services .

Smart cards or similar ideas might be especially useful for providing financial services and access as well as reducing the risk of theft and fraud. Other card-based instruments that have to be considered include:

- Cellular phones, since they remove traditional restrictions of geographical location and high entry costs. With the rapid expansion of WAP-enabled phones, the Internet will be available to all. Even phones that are not WAP-enabled will be capable of being used as payment instruments.
- Set-top boxes that enable owners of television sets to receive digital television signals. These boxes give users access to the Internet, e-mail and various other interactive channels and could be used to make payments.

The legitimacy and security of electronic money payment systems may make or break e-commerce growth in South Africa: if payment systems are too complex or expose consumers to online fraud and theft, e-commerce may suffer a material blow. The South African financial sector is well positioned, especially with regard to large corporate businesses, to support widespread applications of ecommerce. Steps are also being taken by Government, banks and the private sector to find a common standard for smart cards that will be acceptable both nationally and internationally.

QUESTIONS FOR POLICY CONSIDERATION

1. *What needs to be done to further upgrade and integrate national financial services infrastructure to facilitate ecommerce?*
2. *How can banking services be extended to the broader population to allow electronic payments, credit and funds transfer?*
3. *What types of electronic payment systems and technology are most appropriate and practical? How can these be developed effectively on a national level, in coordination with international industry efforts?*
4. *How should Government support these development efforts, both logistically and financially? Which agencies should be responsible? Are there legislative actions that need to be considered?*
5. *Should non-banking institutions be allowed to issue e-money? How can the Reserve Bank ensure that such institutions are licensed, regulated and prudentially secured?*

MAXIMISING BENEFITS

The positive effects of the Internet permeate every aspect of society from the social, economic, technology, education, health and welfare spheres to business and academia. There is a need to extend these benefits to previously disadvantaged communities and individuals through appropriate policy measures. Most policy debate is geared towards removing barriers; developing strategies that maximise e-commerce opportunities, and designing programmes to spur economic growth.

E-commerce presents unique opportunities for less-developed countries to expand their markets externally and internally. The Internet and other technologies might facilitate low-cost international trade even for small businesses while groups that have been marginalised could gain access to financial services and participate more readily in the domestic economy. The location of commercial business centres may become less relevant as companies and workers conduct effective business from almost any location.

Digital divide pertains to inequalities in ICT's distribution between developing and developed economies. It also refers to the gap in the information sphere between developed urban and under-developed rural parts of a country, including disadvantaged groups. The challenge is narrowing the gap between information "haves" and "have-nots".

Despite evidence of the explosive growth of e-commerce together with its revenue-generation and job-creation potentials, many Governments are concerned about. The e-commerce strategy for South Africa will need to take market and human development, jobs, and education and training into consideration.

QUESTIONS FOR POLICY CONSIDERATION

1. *What policies, programmes or partnerships can Government develop or leverage to support and encourage the growth of local e-commerce, and to enhance its social and economic benefits?*
2. *How successful are South African firms in creating and meeting online demand for goods and services? How should companies position themselves to capture greater market share?*
3. *What steps or interventions are required to systematically expand the pool of e-commerce expertise and help resolve skills-gaps or leakages? What, if any, specific interventions are required to foster entrepreneurship and innovation in the sector? What manner of intervention would encourage participation by formerly marginalised entrepreneurs and women?*
4. *What level of Research and Development is required for SMMEs? What institutional support framework should be put in place to assist SMMEs in the adoption of e-commerce? How could the existing structures be improved to encourage and promote faster adoption of e-commerce by SMMEs?*
5. *What kind of public investment is required to foster industry development for the proliferation of e-commerce?*

6. *What is the potential of e-commerce to create jobs? How can job creation be maximised? What strategies should employers and Government devise to minimise the* effects of *perceived job losses or displacements? How can we leverage the available resources to maximise benefits and harness skills?*
7. *What should be the responsibilities of institutions of higher learning and of the Department of Education in education, training and awareness?*
8. *How could the private sector, in partnership with Government, be involved in the awareness campaign and training programmes?*
9. *What funding options are available other than Government resources?*
10. *How can brain-drain be minimised?*
11. *How should curricula be implemented to accelerate e-commerce?*

TRANSFORMATION TO E-GOVERNMENT

Governments are moving from economies centred around agencies and bureaucracies to those that focus on their functions and the needs of citizens. Electronic government can be defined as Government use of ICT to offer citizens and businesses the opportunity to interact and conduct business with Government by using electronic media. Issues to be addressed are:

- Electronic service-delivery - Government of the future entails a shift to citizen and customer-focussed thinking. Citizens must be able to access public services online.
- E-business for e-Government - Government purchasing of goods and services, and electronic payment.
- Governance, information-sharing and exchange - reducing the number of paper transactions in government operations by using intranets and extranets between departments and employees.
- E-commerce policy - e-Government requires an environment conducive to e- commerce policy.
- Technology behind the scenes - leaders need to understand the capabilities of technology.

Environmental pressures and business drivers necessitate transformation to e-Government. Pressures include shrinking budgets and improved-productivity demands, rapid technology advances, shifts in customer expectations and labour pool limitations. Business drivers include improving customer-focus and service, concentrating resources in core areas and increasing competitiveness. By moving towards e-Government, Government will foster entrepreneurial government based on more businesslike practices.

Given that Government is South Africa's largest purchaser of products and services, e-procurement solutions will present the benefits of reduced prices and lower administration burdens and costs; a shorter acquisition and fulfilment cycle; improved inventory practices and better control over "maverick" purchases.

Implementing e-Government strategy will require a sustained Government-wide effort in collaboration with provinces, municipalities and third-party delivery partners. Departments will have to re-engineer programs and processes while maintaining all other delivery channels. Success will depend on major investments of time and money.

HOW TO ACHIEVE E-GOVERNMENT

To launch Government into the Information Age:

- Government must become a knowledge-based workplace. All public servants must be information / communication-literate to improve work processes, service-delivery and teamwork.
- Government employees need to be committed to e-Government. They must understand e-Government, be equipped with the requisite skills and be willing to implement solutions.
- Government's common Information Management / IT infrastructure must be upgraded, and an integrated and coherent IT strategy formulated. The infrastructure must be well-designed, reliable and scalable.
- Data standards must be developed to ensure interoperability between systems.
- A Government Public Key Infrastructure (PKI) must be introduced.
- All public services suitable for electronic delivery should be identified and re-engineered accordingly. The starting point is an audit of services currently offered by departments and working out the savings if these were offered online.

QUESTIONS FOR POLICY CONSIDERATION

1. *Should specific e-Government targets be set?*
2. *What should Government do to accelerate the transformation to e-Government?*
3. *What Government services do citizens and businesses want online?*
4. *How else can Government harness e-commerce to improve service-delivery?*
5. *How can the private sector contribute to e-Government?*

GLOSSARY OF TERMS

Application: a computer program, which performs a set of tasks forming a defined function or service.

Authentication: a mechanism of using information resources to verify the claimed identity of a party to a transaction or an entity involved in a transaction.

Authorisation: an authentication process whereby predetermined rights, including access to information resources, are granted to users or entities

Bandwidth: measure of the capacity of a communications channel, expressed in bits per second

Broadband: this transmission medium allows transmission of voice, data and video simultaneously at higher transfer rates. Broadband transmission media generally can carry multiple channels.

Browser: software on the client's PC used to fetch/read documents from the Web, display them on-screen and print them, jump to others via hypertext, view images and listen to audio files

ccTLD: country code Top Level Domain refers to a high level Internet Protocol address to identify a country e.g, za for South Africa

Confidentiality: reasonable assurance that online or stored data cannot be viewed and interpreted by any person other than an authorised one.

Connectivity: The capability to provide, to end users, connections to the Internet or other communications networks

Cyberspace: the Internet/ electronic/ digital environment

Certification Authority: a secure third party organisation or company that issues digital certificates used to create digital signatures and public key pairs. Certificate authorities guarantee that the two parties exchanging information are really who they claim to be.

Certificate: a certificate is a public key that has been digitally signed by a trusted authority to identify the user of the public key. SET uses certificates to encrypt for example payment information.

Click wrap contracts: Contracts concluded in an online environment, usually the Internet, where the terms of a contract are set out and "offered" by one party on a website and the other party indicates "acceptance" of those terms by for example clicking on an "accept" button or icon and hence concluding the contract

Copyright: the right to retain or sell the rights to an artistic work. Copyright is a form protection to the authors or "original works of authorship" including literary, dramatic, musical, artistic, and certain other intellectual works.

Cryptography: practice of digitally "scrambling" a message using a secret key or keys.

Device: any electronic gadget with an ability to receive input (via a keyboard, or voice) or give output (via screen, or voice, etc.)

Digital: the representation of data by the bits and bytes of binary code. Vinyl records and cassette music tapes carry analogue media

Digital Divide: a term used to reflect the technological gap between countries that have fully exploited ICT and those that have not. The digital divide is often associated with the resulting gap in terms of economic development.

Digital Certificate: See Certificate

Digital Signature: Digital codes that can be attached to an electronically sent message to uniquely identify the sender.

Domain name: A unique name, which represents each computer on the Internet.

Domain Name System: The technical administration and allocation of domain names

EDI: Electronic Data Interchange - is a de facto standard format for exchanging business data between companies computer application in a standardised form, but usually refers to as proprietary system of delivery.

Electronic Fund Transfer: the electronic movement of money over secure private networks between banks' accounts

Electronic Money: means of retail payments executed over Internet, which leaves other traditional electronic payments outside of its scope. Alongside with most commonly used smart card, the term include: e-cards, trade cards, traditional credit, debit and stored value cards, as well as e-cash, digicash, digiwallet, e-credit, e-loans etc.

Electronic payments system: an array of institutions and mechanisms ensuring the cash flow through electronic communications and timely provision of credit and settlements of debts at much less than traditional system could provide costs

Extranet: a website links businesses to customers, suppliers, etc. for electronic communications.

Encryption: the coding of data for the purpose of security or privacy

Gateway: the link between networks and computers which allows messages to be routed across. Often associated with security measures.

Hardware: the physical pieces of computer equipment needed to make up a system.

Hosting: the storage and maintenance of the data making up the content of Websites.

Hyperlink: a reference link that can be made from a point in one web page (traditionally in blue and underlined) to any other point on any web page on the World Wide Web.

ICT: Information and Communication Technologies a generic term used to express the convergence of information of information technology and communications. One prominent example is the Internet

Information-based economy: refers to a country or region where ICT is used to develop economic foundation and market transactions

Interconnection: The connection with each other of the telecommunications networks of different operators so that signals or services are transported over such interconnected networks.

Intellectual Property: comprise two main branches: industrial property, which is chiefly in inventions, trademarks, and industrial designs and appellations origin; and copyright; chiefly in literary, musical, artistic, photographic and audiovisual works.

Integrity: reasonable assurance that stored or online data which its intended destination without being modified in any unauthorised manner.

Internet: the Worldwide collection of networks communicating through common languages and protocols. Also the basic infrastructure for the new economy over which information can be transferred, transactions made and work done

Internet Service Provider: companies that specialise in linking organisations and Individuals to the Internet as well as providing services to them

Intranets: using the same Internet technology, but hosted by private servers not accessible by the public over the Internet. Companies are using Intranets to facilitate their internal knowledge management, communication, collaboration on projects, HR functions, etc.

IP address: the address which all computers and websites have to have on the Internet

Knowledge-based economy: refers to a country or region where ICT is extensively used to enhance knowledge of society in general so that higher human capital brings further improvement to the economy

Local loop: this portion of the telecommunications network physically connects end users to the central office network and generally is dedicated to that particular user.

Multimedia: an interactive combination of text, graphics, animation, images, audio and video displayed by and under the control of a PC

Public key cryptography: this encryption method requires two unique software keys for decrypting data, one public and one private. Data is encrypted using the published public keys and the unpublished private keys are used to decrypt the data.

Portal: website which aims to be the starting point though which one enters the Web.

Personal data: is any data, which refers to an identified or identifiable individual, which is not otherwise readily available via a public source(s).

Permanent Establishment: a fixed place of business through which the business of an enterprise is wholly or partly carried on.

Repudiation: when a customer in a credit card transaction denies having been a party to that transaction.

Server: usually computer hub of a network, fulfilling servers' functions to client computers connected to it, such as storing files and databases and running applications.

Shrink wrap contracts: Same as click wrap contracts except for the fact that the accept icon is actually a shrinked box containing the actual product or service itself e.g. software. Accepting this type of a contract results in an immediate on-line consumption

Smart Card: card containing memory and a microprocessor, that can serve as personal identification, credit card, ATM card, telephone credit card, critical medical information record and as cash for small transactions.

Software: computer programming which gives the hardware its usefulness through various functions the software can perform.

Teledensity: teledensity refers to the number of telephone lines per 100 people, s rough measure of the ubiquity of the public switched telephone network in a country.

VPN: Virtual Private Network - a VPN is a part of the public Internet to which access is controlled by firewalls and secure tunnels to enable private and secure use by authorised users

Website: pages of information linked to one another by hyperlinks (usually organised around a menu), with the main page (usually including the menu) bearing the domain address. These pages are on a Web server and are accessible from any browser on the World Wide Web.

World Wide Web: a collection of information located in many Internet servers that can be accessed with a browser or by navigating via hyperlinks.

Note