Discussion Paper
on Electronic Commerce Policy

Department of Communications
Republic of South Africa

Issued July 1999

Table of Contents

FOREWORD BY IVY MATSEPE-CASABURRI, MINISTER OF COMMUNICATIONS

Dear Colleague

I am very happy to introduce this discussion paper to you.

We stand at an extraordinary and challenging period in the history of our world. In just a few decades, we have been rocketed into a new Information Society. A society driven by a technology that is taking us, daily, into new ways of being; new ways of understanding our world.

The Information Society has changed our ways of communicating with each other, our ways of receiving and sending information and new ways of working. It offers us new potential for development and progress. In the process, it has thrown up new and demanding challenges. Exciting challenges. Sometimes alarming challenges. Challenges that demand that we think seriously about the new global project and how we view our place in it.

Electronic commerce has created a brand new marketplace in which we must operate. It is, in many ways, a marketplace without conventional rules; a marketplace, indeed, that challenges many of our preconceived notions and practices. It is also a marketplace that may seem to defy regulation. Yet, it requires that we think carefully about its implications, both positive and negative, for our society, our country and our continent.

This discussion paper raises some of the questions and issues raised by E-Commerce. There may be many more. This is why we have opened this discussion to as wide an audience as possible. It is, in particular, crucially important that we include the previously marginalised majority of our people in our discussions and thinking, for this is a debate that affects all South Africans. We hope and expect that all those who will be affected by the E-Commerce will play a role in helping us move forward on some of the crucial issues this paper raises, and others that you may feel to be important.

I thank you for your participation.

Let the debate begin!

Acknowledgements

The Minister of Communications would like to acknowledge the contributions of all individuals and organisations who participated in the production of the Discussion Paper on Electronic Commerce Policy. In particular, she would like to acknowledge the following people:

Government E-commerce Task Group consisting of officials from various government departments/ agencies

- Andile Ngcaba – Director-General of Department of Communications and Chairperson of Steering Committee

- **Members of Steering Committee**

  Building Trust - Prof Alko Meijer
  Establishing Ground Rules - Sudhir Sooklal
  Enhancing Infrastructure - Dillo Lehlokoe
  Maximising Benefits - Dr Bob Day

- **Members of Task Teams :**

  M. Davel
  G. Qwabe
  M. Masemola
  G. Claassen
  D. Mitchell
  K Smith
  C. Boonzaier
  S. Sooklal
  R. Brits
  A. Gillespie
  G. Beyl
  D.W Coetsee
  J. Mpshe
  W.Skowronski
  R. Gerber
  I. Macun
  N.Sibitso
  S.Bisseswar

V. Naidoo
S. Grobler
Y. Dixon
H. Marais
P. Monyeki
P. Smit
M. Matlolane
A. Webb
V. Mthembu
K. Kgobokoe
C. Arnold
T. Joubert
M. Ramatlhaphe

- **David N Townsend & Associates (DNTA**), the consultant responsible for preparing the Discussion Paper

- **Edward Nathan & Friedland (ENF),** the consultant responsible for preparing a Due Diligence report on the status of South African laws with respect to e-commerce issues.

- **CSIR,** in particular **Ela Romanowska**, for support to the Department of Communications

Glossary of Terms

ATM	Automated teller machine
CA	Certification authority
DACST	Department of Arts, Culture, Science and Technology
DNS	Domain Name System
DoC	Department of Communications
DTI	Department of Trade and Industry
EDI	Electronic data interchange
EFT	Electronic funds transfer
EU	European Union
FEDI	Financial Electronic Data Interchange
GMPCS	Global Mobile Personal Communications by Satellite
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IPR	Intellectual property rights
ISP	Internet service provider
ITU	International Telecommunication Union
JCSC	Joint Communications Security Council
MPCC	Multipurpose Community Centre
MPTC	Multipurpose telecentre
OECD	Organisation for Economic Co-operation and Development
PIT	Public Information Terminal
PKI	Public key infrastructure
RDP	Reconstruction and Development Programme
SABS	South African Bureau of Standards
SACSA	South African Communications Security Agency
SAIDI	South African Integrated Development Initiative
SAITIS	South African Information Technology Industry Strategy
SAMOS	South African Multiple Option Settlement
SATRA	South African Telecommunications Regulatory Authority
SBC	Southern Bell Corporation
SMME	Small, medium and micro enterprises
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TRIPS	Trade-related aspects of intellectual property rights
TTP	Trusted Third Party
UNCITRAL	United Nations Commission on International Trade Law

UNCTAD	United Nations Conference on Trade and Development
URL	Uniform Resource Locator
US	United States of America
USA	Universal Service Agency
USF	Universal Service Fund
WIPO	World Intellectual Property Organisation
WTO	World Trade Organisation

South Africa Department of Communications
Discussion Paper on Electronic Commerce

1. Introduction

This Discussion Paper has been prepared on behalf of the Department of Communications (DoC) of the Republic of South Africa to serve as a starting point for national policy discussions concerning the development of Electronic Commerce in South Africa. The paper is the result of extensive collaborative efforts by an initiative set up under the direction of DoC, with participation by a wide range of representatives of various government departments and agencies. The stakeholders and participants in the initiative thus far are listed under Acknowledgements at the beginning of this document.

The purpose of this paper is to present background and summary discussion of the many policy issues surrounding e-commerce, as a foundation for national deliberations on how best to formulate a coherent policy strategy. The various topics are discussed both from a general point of view and from the perspective of current policy and initiatives in South Africa, which might be expanded or adapted for incorporation into a national policy.

Background information used in the development of this report includes –
- reference documents and websites (see appendix 1);
- extensive documents produced by the four government task groups, defined according to the action plan of the Organisation for Economic Co-operation and Development (OECD); and
- inputs from consultants, including a legal due diligence investigation on potential barriers to electronic commerce presented by South African laws (statutory and common law).

Detailed references to the above sources are available from the DoC on request.

What is electronic commerce?

Electronic commerce (or e-commerce) encompasses all business conducted by means of computer networks. It reflects a paradigm shift driven by two primary factors:
- a wide range of converging technological developments and
- the emergence of the so-called “knowledge economy”.

When communications networks first became available, entrepreneurs were quick to recognise their value and use them to create business opportunities. Recent advances in telecommunications and computer technologies have moved computer networks to the centre of the international economic infrastructure. Most prominently, the meteoric rise of the Internet and the World Wide Web has transformed global commerce by facilitating instantaneous, inexpensive contact among sellers, buyers, investors, advertisers and financiers anywhere in the world. The rapid integration of Internet and other telecommunications-based functions into nearly every sphere of business has led to an international focus on the new world of e-commerce.

These technological developments have gone hand in hand with a trend, predominantly in the developed world, towards a post-industrial knowledge economy. This new paradigm, which is already having a significant impact on the way in which people lead their lives, is difficult to define but is characterised by –
- an emphasis on the human mind, rather than merely physical automation;
- being information- rather than energy intensive;
- sustainability through networks, not single organisations;

- supporting distributed rather than centralised intelligence;
- requiring multiple skills and continuous learning;
- replacing lifetime employment with labour market flexibility;
- customised rather than standardised products; and
- being enabled by information and communications technologies (ICTs), whilst simultaneously driving the development of new ICTs.

Just as the industrial society built on and then dominated the agricultural society, the knowledge society is now building on the platform provided by the industrial society. It can be argued that e-commerce, along with the technologies and knowledge required to effect it, is the first real manifestation of the knowledge society. The question for the less industrialised developing countries is whether they can use appropriate technologies to leapfrog into the knowledge society, by-passing some of the stages of the industrial paradigm.

Among the principal activities that can be identified as contributing to global e-commerce are –
- government services and information;
- business-to-business wholesale and retail services and sales;
- business-to consumer (and consumer-to-consumer) retail sales and transactions;
- financial services and transactions;
- subscription and usage-based telephony, online and Internet access services;
- subscription or transaction-based information services and software sales;
- advertising and marketing services; and
- ancillary functions contributing to business/commercial activities.

The vast majority of these transactions to date have been taking place in countries with advanced economies and infrastructure, such as the members of the Organisation for Economic Co-operation and Development (OECD). For developing countries like South Africa, e-commerce presents important new opportunities to achieve a more level playing field vis-à-vis larger, more developed economies: it diminishes existing advantages of cost, communication, and information, and can create huge new markets for indigenous products and services. While many companies and communities in South Africa are beginning to take advantage of the potential of e-commerce, critical challenges remain to be overcome before its potential can be fully realised for the benefit of all citizens.

Content of this report

The sections that follow discuss the main areas of policy debate on e-commerce, using the subject classification adopted for the Task Groups of the South African National Government Electronic Commerce Initiative (SANGECI). These classifications roughly follow the categories defined by the OECD at its recent series of international conferences on e-commerce. These categories identify potential barriers to e-commerce development and strategies for its promotion. In addition, there are two introductory sections concerning the overall philosophy and policy co-ordination on e-commerce in South Africa. The specific topics covered are:

- **Philosophy** (Section 2) What should be the governing philosophy that guides nation-wide decisions on priorities and options concerning e-commerce development? This section proposes a basic set of principles.

- **Policy co-ordination** (Section 3) For policy on e-commerce to be effective, a myriad different initiatives and activities in the public and private sector need to be effectively co-ordinated. The key question is how and under what organisational structure this can best be done.
- **Building Trust** (Section 4) Discussion of policies to help overcome real and perceived risks to businesses and consumers that can arise in electronic transactions.
- **Establishing Ground Rules** (Section 5) Discussion of policies that define the common rules and practices applicable to electronically based businesses, on a national and international level.
- **Enhancing Infrastructure** (Section 6) Discussion of policies for enhancing the information, telecommunication and financial services technologies and facilities that are essential for participation in global e-commerce.
- **Maximising Benefits** (Section 7) Discussion of policies that focus on promoting new business opportunities and on easing the transformation of the economy.

2. Philosophy

The objectives for a national policy to support and expand e-commerce in South Africa should be based upon a clear and coherent set of underlying principles. Policies in a variety of sectors must be harmonised according to this overall philosophical framework to ensure that the country and its citizens benefit optimally from the transformation of the economy. This section offers a Draft Statement of Principles suggesting a framework for such an overall philosophy. It is based on two interconnected objectives: improving quality of life, and equitable development.

2.1 Quality of life

The overriding purpose of the government of the new South Africa is to establish policies and practical programmes that will improve the quality of life for all South Africans. This fundamental objective should also serve as the guiding philosophy for the establishment of South African e-commerce policies.

The concept of quality of life embraces many dimensions, and may be different for different people. In pure economic terms, it implies income and purchasing power; employment opportunities; access to essential resources such as food, clothing, and shelter; and the potential for upward mobility toward greater wealth and comfort. It also implies a degree of choice in individuals' economic options, both in employment and in consumption. Beyond economics *per se*, quality of life also implies certain other basic rights and human needs, many of which can be directly affected by the new technologies and relationships that arise with e-commerce. Some examples of these conditions that bear discussion, and the related opportunities and risks presented by e-commerce, include –

- **good health**, long life, the absence of disease, and access to effective health care (Opportunity = Tele-medicine, access to on-line health information; Risk = possible adverse health impacts of excessive computer usage);
- **basic and advanced education**, from literacy through secondary school, job and skill training, and advanced learning for both career and personal enrichment (Opportunity = distance learning and electronic training; Risk = possible increase in disparities between computer literate and unskilled);
- **democratic participation**, including awareness and exercise of political rights, access to government information and services, opportunity to contact and influence public agencies and to promote decentralisation (Opportunity = access to government information, electoral websites; Risk = misuse of technology for propaganda);
- **cultural expression**: the preservation and nurturing of indigenous languages, customs, arts and traditions (Opportunity = unlimited new channels and affordable means for individual expression; Risk = domination of media by the few with most resources);
- **family and community cohesiveness**: the opportunity to sustain and enjoy these relationships without sacrificing economic choices (Opportunity = long-distance, low-cost multimedia communication; Risk = dehumanisation of interaction; individualising effects of technology);

- **religious and spiritual fulfilment**: free practice and expression of beliefs and rituals, and opportunity to explore spiritual growth in an uninhibited manner (Opportunity = greater means for expressing and sharing experiences and beliefs; Risk = distortion or suppression of experience by technology);
- **entertainment** and leisure options, including the time and means to enjoy them (Opportunity = limitless access to multimedia entertainment sources; Risk = cost, fixation with technology-based media, proliferation of low-quality or undesirable material); and
- **personal liberty, safety, and privacy**: freedom from oppression, domination, and risk of war or crime, as well as protection from invasions of privacy by either governments, businesses, or individuals (Opportunity = ability to expose oppression, share experience, learn self-protection; Risk = exploitation and privacy violations via technology).

All of these conditions are aspects of quality of life, though not all citizens would agree as to their relative importance. Certainly not every policy or practice associated with e-commerce will affect all or even most of these dimensions. What is important to recognise is that some policies are likely to have differential impacts in several areas: a given policy may improve some aspects of life for some groups while neglecting or diminishing other aspects for the same or different groups.

The first challenge is to identify and understand the potential consequences of the transformation of economic and social activities, and to consider all elements of those changes when determining the best path. Where tradeoffs cannot be avoided, it is important that the gains and losses in different areas be weighed on a society-wide basis, and that the ultimate choices be transparent, fair, and clearly justified.

2.2 Equitable development

Improving the quality of life for citizens implies moving from the status quo toward a condition that is better to some degree. But the status quo, in terms of quality of life, is radically different for different groups of South Africans. We are not simply concerned with bettering the position of each South African in equal measure. Rather, the policy objective of improving quality of life in South Africa must necessarily be disproportionate in its focus, to help rectify historical inequities in both economic and non-economic circumstances among major segments of the population. However, the broader and longer-term goal is for nationwide (and region-wide) growth for the whole of society.

As technology expands to allow increased integration and participation of all consumers in the economy, it may be that one of the most effective means for achieving national economic growth is to focus public and private resources on those populations that have been most excluded from economic participation. Empowering disadvantaged communities and raising their living standards not only benefits those target groups directly, it yields tangible benefits to the entire national economy. Such benefits include increased productivity, an expanded marketplace for businesses, diversity of experience and ideas contributing to development, reduced costs of poverty and distress, and many other positive effects.

The goals of improvement in quality of life and overall economic growth are thus inextricably linked with the principles of social equity. We can therefore define the ultimate strategic objective of policies to support e-commerce to be "equitable development". Development is required to

achieve equity, and equity is a key means to spur development. The five principal policy thrusts underlying this objective are as follows:

- eradication of poverty;
- alleviation of historical disadvantages;
- economic growth;
- global competitiveness; and
- promotion of a post-industrial society.

These principles should underlie all considerations of specific policy options relating to the development of e-commerce in South Africa. In some cases, the primary objective of encouraging general economic growth and opportunity may directly support a certain set of policies. In other circumstances, however, the nuances of policy options may require that their potential impact on the equitable distribution of opportunities be reviewed and the benefits of e-commerce for impoverished and disadvantaged populations be given greater emphasis.

It is important to remember and be aware of these subtle distinctions since they are rarely noted in the international e-commerce literature and precedents, which have been created largely in the United States and Europe. If South Africa is to establish a policy of improving the quality of life for all its citizens through equitable development, and thereby set new precedents for the role of e-commerce in the less developed countries of the world, it must adhere closely to these principles while nevertheless maintaining the broad focus on fostering widespread economic growth, opportunity and global integration.

3. Policy Co-ordination

One theme has become apparent throughout the discussions and research that have contributed to this policy review process for South Africa: that effective development of e-commerce opportunities will depend heavily on a co-ordinated, participatory process that involves a wide range of stakeholders in both the public and private sectors. Electronic commerce involves the integration of many elements of technology, infrastructure, business operation and public policy, which need to operate as smoothly as possible together to yield the maximum benefits to the public. Naturally, the technologies need to be fully operational, and the legal and business environment needs to favour entrepreneurial and innovative approaches to market development. As the policy issues discussed in the subsequent sections of this paper demonstrate, these requirements cut across private and public sectors, and all sectors of the society.

An effective national policy on e-commerce can be established only if disparate operational, legal, regulatory, and enforcement actions within the government, along with technical, marketing, financial, and management strategies in the business sector, are closely aligned. Success depends upon two main factors: active **participation** in policy deliberations by all stakeholders, and co-ordinated **leadership** of strategic policy development to ensure common goals and approaches on all sides.

The appropriate leadership responsibilities should be determined in a policy decision from the highest levels of government, with as much consensus as possible from all affected departments. The Department of Communications should be in the best position to co-ordinate and understand the various issues and initiatives, particularly in the crucial areas of infrastructure which must underlie all e-commerce development. The South African Law Commission also has a crucial role to play in speeding up the process of formulating policy and defining new legislative initiatives.

The government departments that should be involved in defining and implementing South African e-commerce policies encompass nearly every agency in some way or another. Many offices have participated actively in the process of policy review that led to this Discussion Paper. The following are some of the key areas in which government departments and other bodies can contribute to the development of a national e-commerce policy:

- **Department of Education**: Overall education policies on information technologies; distance learning programmes;
- **Department of Labour**: Programmes on skills training, technology job placement, policies on industry evolution;
- **Department of Health**: Tele-medicine programmes, health information database and education initiatives;
- **Department of Trade and Industry**: World Trade Organisation (WTO) negotiations, imports and customs issues, harmonisation of South African policy with global treaties, and local industrial strategies, particularly the South African Information Technology Industry Strategy (SAITIS) project;
- **South African Bureau of Standards**: The establishment and management of standards;

- **Department of Finance, South African Revenue Service**: Policies on tax treatment, revenue collection for electronic transactions and imports and customs issues;
- **South African Communications Security Agency (SACSA):** Policies on cryptography including digital signatures, certification authorities, public key infrastructures;
- **Department of Arts, Culture, Science and Technology (DACST)**: Policies relating to development of technology, particularly the information and communications technology (ICT) sector of the national research and technology foresight project, as well as cultural expression via new technologies;
- **Department of Justice, National Intelligence Agency**: Investigation and prevention of cyberfraud, illegal transmissions and other security threats; establishment of information technology security policies for government;
- **Department of Public Service and Administration**: Establishment of information technology and information management policies for government;
- **Department of Public Works**: Electronic archiving policies and strategies;
- **Department of Home Affairs**: Development of a national identity card with a smart chip catering for various uses;
- **South African Reserve Bank**: Initiatives on electronic payments, funds exchange, inter-bank technologies and electronic money.

4. Building Trust

One of the main differences between e-commerce and traditional commerce is that electronic transactions are far more impersonal, anonymous and automated than transactions made between flesh-and-blood persons in a store, at a bank or even over the telephone. This dehumanisation of business relations is accompanied by an increase in the technical means and opportunity for fraud and abuse of individual consumers and large corporations alike. For all these reasons, a healthy sense of caution, if not outright distrust, has prevailed in the evolution of many aspects of e-commerce.

Moreover, on-line merchants and consumers all over the world are discovering that the rules and laws of conventional commerce become strained in their application to the digital environment. This lack of legal certainty contributes significantly to the prevailing sense of caution.

Consequently, for these new, globally impersonal technologies to advance to a more universal level of acceptance, business and government institutions must develop policies that build greater trust in the new transaction media. Trust implies confidence –

- that electronically-based purchases, funds transfers and business deals will be as valid as traditional activities;
- that personal information and finances will be secure;
- that consumers will be protected from fraud and mistreatment; and
- that the world of on-line information and communications will be at least as accountable for the quality, reliability, and legality of products and services as is the in-person world.

The principal elements of trust in the context of on-line commercial transactions can be classified as follows:

- **Security**: Confidence that information transmitted during a transaction will arrive in uncorrupted form and will not be improperly leaked to others; this category thus encompasses both the *integrity* and the *confidentiality* of data transmissions (see 4.1, Security of data transmissions).
- **Privacy**: Concerns about access to and use of personal information obtained directly or indirectly as a result of electronic transactions (see 4.2, Privacy protection).
- **Authenticity**: Verification that the parties to a transaction, and the services rendered, are truly as represented (see 4.4, Certification authorities, and 4.5, Consumer protection).
- **Non-repudiability**: Assurance that a transaction will be honoured as agreed, and that each party can prove, in a court of law if necessary, the validity of the terms of the deal without opportunity to renege (see 4.3, Digital signatures and electronic contracts).

The topics in this category are closely linked. Issues of security and cryptography tie in with both privacy protection and certification, as well as with the technical options for creating and validating digital signatures. All of these concerns relate to consumer protection as well as to ensuring the integrity of on-line business and government activities.

4.1. Security of data transmissions

Complex security problems confront global information networks. Governments and businesses are grappling with the need to secure geographically dispersed networks, myriads of access points, and business-critical applications against theft, fraud, abuse and even electronic terrorism.

The need to maximise the benefits of universal connectivity while protecting network resources from unauthorised access or interference has fuelled a heightened demand for global network data security solutions. Recent experience with e-mail-based viruses has further reinforced these concerns.

A number of countermeasures are already being taken to ensure that e-commerce is as secure as traditional forms of transaction. Encryption is an essential tool in providing security in this highly-networked environment. Highly secure encryption can be deployed fairly cheaply, and it is expected that encryption will be broadly adopted and embedded in most electronic communication products and applications for handling valuable data. Applications include protecting files from theft or unauthorised access, keeping communications secure from interception, and facilitating secure transactions. Cryptography can also be used to guarantee integrity (i.e. that the contents of a file or message have not been altered), to establish the identity of a party, or to make legal commitments.

The widespread use of cryptography raises a number of issues, particularly for governments. These include protection of citizens' privacy, encouraging economic well-being, maintaining public safety, raising revenues, and facilitating law enforcement and national security. Although there are legitimate commercial and individual needs and uses for cryptography, it may also be used for illegal activities detrimental to public safety, law enforcement, business and consumer interests, and privacy.

Because encryption technology is becoming so widely available and affordable, it would be impractical for governments to attempt to prohibit its use altogether, and such a policy would be highly detrimental to consumer confidence in electronic transactions. It may be appropriate, however, for the government to consider certain limits and requirements for encryption, such as restrictions on the complexity of encryption. Some countries also place restrictions on the export of encryption technology. This issue could be raised, for example, if South Africa were to consider becoming a signatory to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies [1]. If the South African software industry were to develop unique and commercially viable new encryption technologies, however, any export limitations could inhibit the growth of this industry.

An important issue that arises as the use of encryption spreads is the means and extent of *lawful access* to cryptographic codes (or decryption keys) by government agencies such as law enforcement and national security. For decades, security agencies have considered the interception and decryption of communications a central tool of national defence; the US government therefore classifies cryptographic equipment as war munitions and places tight controls on its export. The same techniques have become increasingly prominent in response to terrorism and other global security threats. Similarly, domestic law enforcement agencies have often relied on wiretapping and other surveillance of communications, both to prevent crime and to establish evidence for the prosecution of criminals.

Because of these public interests, security agencies have advocated that limits be placed on the sophistication and availability of encryption technologies and/or that they be given access to encrypted transmissions. There are generally three approaches that can be considered to provide some degree of access for law enforcement authorities to encrypted data and communications:

- weak cryptography;
- key escrow; or

- direct access to session keys.

Weak cryptography would require data encryption algorithm key lengths to be limited to, say, less than 40 bits, to allow security agencies to decrypt transmissions, preferably in real time. While this approach would arguably yield the most effective means of monitoring suspect transmissions, it would also increase the vulnerability of legitimate communications. In practice, it would also be difficult to enforce, especially among those elements (criminals, terrorists, etc.) who would be the primary focus of such surveillance.

The other two options for access to encrypted data depend on some form of access to the decryption keys associated with each particular transmission or database. *Key escrow* implies a system in which the decryption keys for all cryptographic codes are made available to a designated government agency. Under a proper court order or other legal mandate, this agency would provide a given key to a law enforcement office, which could use it to monitor or read suspect data transmissions. The main objection to this policy is that, once given the key, the law enforcement authorities could read *all* transmissions of a particular user, not only those subject to the court order.

Direct access to session keys would involve direct interaction between the authorities and users, obligating users to turn over their own keys upon receipt of a warrant or court order. Refusal to provide the key would itself be a criminal offence. A likely variation on this approach would be a situation where corporations outsourced their encryption functions to a so-called “trusted third party” (TTP), which would be the *de facto* holder of the keys. Keys could also be held by certification authorities (CAs, see below). TTPs and CAs could represent a more clandestine means of access to sensitive data, without directly alerting users that may be under surveillance.

One concern regarding these proposed arrangements is that TTPs themselves could be vulnerable to corruption, infiltration or abuse. In addition, the set of responsibilities and relationships created by these complex access obligations will inevitably add considerable cost to corporations’ data-processing and communications functions.

There is currently no international consensus on ways of maintaining trust in data security while allowing some degree of lawful access to digital transmissions. The range of policies in Europe, for example, includes –

- no official stance (a “wait and see” policy, as in Denmark and Germany);
- key access obligations (Council of Europe recommendations);
- voluntary licensing of CAs and TTPs (United Kingdom);
- obligatory weak cryptography and key escrow (France, discontinued in January 1999).

Current policy and initiatives in South Africa

Current legislation relating to security of transmissions in South Africa includes the *Interception and Monitoring Prohibition Act of 1992*. Amendments to this Act have recently been proposed, but it remains unclear to what extent they will directly address issues specific to data transmission and security. The Act appears to be aimed mainly at traditional voice communication, to prevent unauthorised interception of, for example, cellular telephone calls.

The proposed amendments would require telecommunications operators to provide means for law enforcement agencies to intercept and monitor communications – apparently including e-mail – under a suitable court order. Specific issues of access to encryption keys have not been

addressed, nor has the technical feasibility of the types of monitoring that would be needed in a digital transmission environment.

Questions for policy consideration

South Africa has to consider its stance with regard both to promoting the benefits of increased data security and to ensuring that law enforcement agencies will be able to investigate criminal and other illicit transmissions. These deliberations must also take into account the various policies of other countries and the role that South Africa wishes to play in promoting uniform standards internationally.

- Should South Africa adopt specific policies and legislation at this time to encourage and/or restrict the use of encryption in commercial data transmissions?
- To encourage greater public confidence in e-commerce, should the South African government officially endorse certain cryptographic methods, or TTP/CA institutions? (See also Section 4.4.)
- What restrictions, if any, should be placed on the use and sophistication of cryptography in domestic businesses' electronic transactions?
- Should government law enforcement agencies have access to public keys to private cryptographic technology? What rules should apply and which institutions should be involved?
- How should South Africa participate in international deliberations and agreements toward common standards for cross-border data security and access?

4.2 Privacy protection

As distinct from concerns about data protection and security for commercial purposes (e.g. to prevent theft), there is a larger area of concern regarding individuals' rights to privacy in the electronic age. The technology of the Internet has made it increasingly easy to obtain detailed, personal information about users, without their knowledge or consent. Of particular sensitivity is information in three categories: medical, financial, and child-related. Many websites routinely, and often unscrupulously, ask users for personal information in these and other areas. Having once given it, the user cannot tell how it will be used or to whom it might be made available. Other data, specifically associated with the user's web browser and originating URL (address), is often automatically collected when users enter a location. These types of data can be of great commercial value to marketers and others, but also have the potential to be abused in a variety of ways.

There is consequently a strong move in favour of establishing new, clear rights and laws to prevent unauthorised use and dissemination of personal data, and otherwise to assure some degree of control over access to private information, and invasions of privacy generally.

Some 50 countries have adopted legislation and self-regulatory measures that require government and private sector organisations which maintain systems of name-linked records to observe "fair personal information principles and practices".

The Internet has raised new issues concerning confidentiality of records in terms of access to personal details, jurisdiction over storage and use of data, and protection of financial information

disclosed in electronic transactions. The degree of mandatory versus voluntary regulation of personal data is one issue of contention, as is the practical enforceability of privacy standards. These concerns apply not only to transmission media, but also to computer software, which, as recent experience has shown, can incorporate revealing information about users without their knowledge.

In general, there are four main approaches that can be considered for enhancing users' sense of privacy protection in the on-line environment:

- **Government regulation** through specific legislation, to require website operators and database owners to conform to certain standards regarding the use of data;
- **Self-regulation** within the industry, with voluntary standards for disclosure of data collection and usage policies;
- **Informed consent**, which can either be mandated by law or agreed voluntarily, and which involves specific standards for informing users of how their personal information might be used and for obtaining explicit consent to such use in advance; and
- **Technological approaches**, such as filters that allow parents to limit their children's access to certain websites, and other software options that are being developed to give consumers greater control over access to their personal data.

The notion of *informed consent* mentioned above appears to enjoy broad support as a basic principle for the handling of personal data on the Internet and in other contexts. The main debate focuses around the extent to which this principle should be enforced through legislation and government regulation, as opposed to self-regulatory standards. A general informed consent policy typically consists of the following elements:

- **Notice** of a company's or website's policies and practices with respect to the collection, use, and dissemination of consumer data should be prominently posted; this should also include clear identification of the entity collecting and storing the data.
- Consumers should have a clear **choice** as to whether their personal information can be used in any manner; moreover this must be an affirmative decision, rather than "passive" approval (i.e. failure to disapprove).
- Users must have a right of **access** to whatever information a company may hold on them, and the means to correct or modify (or remove) any information that is faulty, or that the consumer doesn't wish the database owner to retain.
- Specific descriptions of the **security** policies and practices of the database owner should be available for scrutiny by all users.

Much of the debate over the issue of self-regulation versus government regulation has played out between the United States and the European Union. The US government has, for the most part, emphasised the self-regulation principle, reflecting concerns that government intervention could inhibit the legitimate collection and use of commercially valuable data and add excessive costs and burdens to on-line commerce. The EU, on the other hand, has favoured a strong regulatory approach, which is encompassed by its *European Data Protection Directive* [2, 3]. This directive requires that EU nations adopt a set of standards similar to those listed above, and moreover that

no data may be transmitted from any EU country to another country that does not "ensure an adequate level of protection" of personal data in a similar manner.

Current policy and initiatives in South Africa

Section 14 of the South African Constitution of 1996 states:

> *"Everyone has the right to privacy, which includes the right not to have*
> *(a) their person or home searched;*
> *(b) their property searched;*
> *(c) their possessions seized; or*
> *(d) the privacy of their communications infringed."*

Section 32 of the Constitution states:

> *"(1) Everyone has the right of access to:*
> *(a) any information held by the state; and*
> *(b) any information that is held by another person and that is required for the exercise or protection of any rights;*
>
> *(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state."*

Such legislation to protect privacy as intended by these clauses has not yet been passed by the legislature. The Open Democracy Bill was introduced in July 1998, but has been withdrawn. The draft contained provisions to allow individuals access to, correction of, and limits on use of personal information, to be enforced by the Human Rights Commission.

Questions for policy consideration

It appears that some degree of more precise legislation in support of consumer privacy protection is warranted in South Africa, with particular emphasis on electronic communications. Among the key questions that should be considered are the following:

- Should South Africa adopt specific requirements for database owners and others collecting personal information, with regard to the treatment of such data?
- To what extent should companies be allowed/encouraged to adopt self-regulation standards for privacy protection?
- Should there be official minimum requirements for notice, choice, access and security practices concerning data collection and use?
- What penalties should be imposed for misuse of personal data, either by collecting information without consent, selling or distributing unauthorised data, or other abuses?
- If direct government regulation is to be considered, which bodies (e.g., the Human Rights Commission or a new agency) should be responsible for monitoring and enforcing privacy rules? What powers and limitations should such an agency have with regard to examining companies' databases and practices?

- What role should other consumer protection bodies (e.g. the Consumer Council) play in this regard?

4.3 Digital signatures and electronic contracts

Many aspects of building trust involve an overlap of legal and technological issues. This applies particularly to the changes in contractual relations between businesses. Most contract law has been designed to govern traditional economic relations, consummated using traditional media, i.e. paper documents. The nature of electronic deals complicates these relations by raising questions about precisely how electronic "virtual" documents and/or signatures are covered by these laws.

Hand-written signatures have been universally accepted for centuries as binding evidence of commitments – an essential pillar of business dealings. The notion of "digital signatures", in which a commitment is sealed via an imprint of electronic bits rather than pen and ink, involves more than just a shift in habits. It requires commonly recognised protocols, means for detecting digital forgery, and standards for verifying the timing of correspondence and the integrity of data files that can be readily manipulated, changed, and deleted without leaving a "paper trail".

There are a great many nuances to the legal definitions and implications of the use of digital or electronic signatures, in combination with encryption, key access, and certification practices. In principle, existing laws may need to be expanded, or new laws written, to ensure that provisions that have traditionally applied to written signatures can be applied with equal reliability to digital signatures. A directive of the European Union identifies some of the main issues involved in the legal recognition of digital signatures:

- **Declarations of intent**: A signature is traditionally accepted in contract law as a binding declaration of the intent of the signer. However, the conditions of electronic communication, including the ability to transmit information instantaneously and in multiple forms, may cloud the certainty of the user's intent as conveyed in electronic documents.
- **Non-repudiation**: The reliability of signatures is tied to the ability to verify the identity of the signer, which has traditionally depended upon the uniqueness of hand-written signatures. With sophisticated encryption and key escrow technologies, such uniqueness may not exist, and actual digital signatures may not even be directly applied by users. The law needs to be able to determine validity in these circumstances, along with limits to liability for "false" signatures.
- **Legal treatment of references**: In paper documents such as contracts, incorporation of other documents or policies by reference implies specifically identifiable and verifiable terms and conditions. When similar material is incorporated by reference electronically (e.g. by pointing to a website), the integrity and validity of the referenced material may be less certain. The law needs to define standards for legal treatment in these cases.
- **Legal effects**: Again, traditional reference to documents in many laws needs to be reviewed to incorporate the differences that arise through the use of electronic documents. This includes the recognition of documents as evidence in legal proceedings, and stipulation as to when an electronic document can be treated as equivalent to a written form.

In an attempt to tackle the many questions that arise in the context of electronic contracts and digital signatures, the United Nations Commission on International Trade Law (UNCITRAL) has

drafted an extensive Model Law on Electronic Commerce. UNCITRAL has offered this Model Law to the world's governments as a proposed framework for the consideration of these issues, and to help to harmonise their legal treatment worldwide. The objectives of the Model Law are to facilitate the use of such communications techniques as electronic data interchange (EDI) and electronic mail, and to provide for equal treatment of users of paper-based documentation and users of computer-based information, which is essential for fostering economy and efficiency in international trade. Other draft proposals for similar legislative initiatives have been issued by the International Chamber of Commerce and the American Bar Association.

Current policy and initiatives in South Africa

It is generally acknowledged that, like most countries, South Africa does not at this time have a legal framework in place for addressing electronic contracts or digital signatures. The existing guidelines by the South African Bureau of Standards (SABS) can be found in documents entitled: Recommended practice ARP 044 Model interchange agreement and SABS 1621 African standard.

The issues raised in this context could be addressed by the South African Law Commission, possibly in conjunction with its initiatives to develop legislation regarding computer crime.

Questions for policy consideration

- If the current South African legal environment needs to be revisited, should the so-called "legal barriers" to contracting by electronic means be addressed by –
  - leaving the matter to the courts to clear up?
  - referring the matter to the Law Commission to investigate and make recommendations?
  - amending the Interpretation Act 33 of 1957?
  - amending individual pieces of legislation?
  - adopting the provisions of the UNCITRAL Model Law in an Act specific to electronic commerce?
  - a combination of the above?
- Should legislative intervention in the form of an electronic commerce-specific Act be favoured, is the UNCITRAL Model Law adequate to adapt to the legal treatment of contract law in South Africa? What modifications or adjustments might be necessary, and which issues other than contracting, evidence and digital signatures should be incorporated?
- Should legislative intervention based on the UNCITRAL Model Law be initiated as a matter of urgency, separate from other issues such as consumer protection, taxation, intellectual property, infrastructure, etc.? If so, should the Law Commission be charged with the legislative process or should it be handled elsewhere, e.g. the Department of Communications and/or the Department of Trade and Industry?
- What other aspects of existing law which may be relevant to electronic commerce need to be revisited, and by whom, to make them compatible with the demands of electronic commerce?
- How compatible are South African laws with those of other countries in Africa and elsewhere, and what steps should be taken to harmonise these laws so that companies can operate in a predictable and stable international business environment? In particular, should

South Africa adopt the OECD position that digital signature laws should not "require localisation" but should simply be based upon neutral criteria, so that they will not form trade barriers?

4.4 Certification and certification authorities

In any commercial transaction between two parties it is essential that each party is certain about the identity of the other. Such certainty can be obtained through the use of public key cryptography, in which the recipient's public key is employed in encrypting data, and the sender's private key is used for signing, and the sender's public key is then used for verification of the sender's signature by the recipient. However, since a public key is merely a long string of bits, successful verification of a signature is not sufficient to bind the sender's identity to the public key. A dishonest party can publish a public key (to which only it has the corresponding private key), while claiming to be some other party, perhaps one with a reputation for sound and honest business practices. Some process of binding the identity of an entity to its public key is therefore necessary. Such a service can be provided by one or more trusted third parties.

In what appears to have become the most widely used infrastructure, commercial and/or government organisations called certification authorities (CAs) are set up to certify the public keys of individual entities. This is done by issuing public key certificates, which are in essence digital certificates containing the name of the holder of a public key along with that particular public key, the whole certificate being signed by means of the CA's private key. In this way, the trust in a signature is transferred to the trust placed in the CA who signed the certificate, or at least in its public key.

In its turn, the public key of a CA can be certified by another CA at a higher level, or, in order to keep the structure manageable and key verification more efficient, CAs can cross-certify each other's public keys. The resulting system of CAs and their mutual certifications is known as a public key infrastructure (PKI).

The Task Group on Building Trust for Users and Consumers, following the Canadian example, has discussed a PKI in which a government agency would issue and certify public keys for government agencies, while commercial CAs would do the same for commercial and general non-governmental purposes, with some degree of cross-certification between these.

CAs may, of course, also perform other cryptography-related functions, such as message key archiving on behalf of its users. Whatever services they provide, the most important one is the certification of users' public keys. Users must therefore be able to place a great degree of trust in the CAs, and consideration needs to be given to the criteria on which such trust can be based.

Both the United Nations and the European Union have issued detailed criteria for the makeup and activities of certification authorities. In general, certification authorities should –

- be reliable enough to offer certification services;
- employ personnel with appropriate skills and qualifications;
- use trustworthy systems, including approved hardware and software;
- have sufficient financial resources;
- publish all relevant information concerning their procedures and policies, both for certification and for complaints and dispute settlement.

One of the main policy debates surrounding private sector CAs is whether they should require formal licensing by the government or whether self-regulation without official endorsement should be allowed. In view of the potential importance of CA activities, the large amounts of money that could be involved in many transactions, and the potential liability questions that could arise, public licensing may be necessary. The opposing view contends that the hierarchy of licensing, government certification, and industry CAs could stifle e-commerce in red tape.

Licensing of CAs need not necessarily be mandatory. A licensing regime would obviously offer strong reassurance to the public that licensed CAs are reliable and responsible, but self-established (unlicensed) CAs might still be allowed to compete for public confidence. In particular, in-house CAs within companies might not need to be licensed; when outside vendors or partners rely on their services, liability can be covered through contract terms.

Where CAs are to be licensed, it will be necessary to define general policies applicable to CAs and to appoint an official agency to issue licenses and monitor compliance with the policy standards. The policies that need to be defined include the relative liability of CAs, their legal responsibilities, public reporting requirements, organisational and personnel standards, and the range of activities and expertise they may provide. These policies may be established explicitly through legislation or can be defined by an authorised government regulator under legislative principles. In either case, their design and implementation should be based on substantial input from affected industry participants. The ultimate licensing and certification processes, however, should be clearly independent of vested interests.

Finally it is vital, in a globally connected marketplace, that national policies for certification be harmonised as far as possible with those of trading partners, so that trust can be reinforced for international trade as well as domestic transactions. This implies both technical *interoperability* of cryptographic and key access technologies (including recognition of digital signatures), and common standards and policies for certification and disclosure of information. To achieve this objective, it may be necessary for South Africa to pursue bilateral or multilateral treaties that define mutual recognition of certification authorities and procedures. Technical standards for certification are likely to be established on a global level, e.g. by the International Telecommunication Union (ITU) or industry groups, just as global policies and agreements are likely to be negotiated via the WTO and regional bodies. South Africa should maintain contact and monitor progress in all these areas.

Current policy and initiatives in South Africa

As policy and practice regarding certification authorities and public key infrastructure issues are very new worldwide, no specific framework yet exists in South Africa to promote these policies. A few private sector CAs have been set up, notably in the banking industry, but without any official licensing or validation. According to the Task Group, the Joint Communications Security Council (JCSC) would be in a position, with industry input, to support the definition of licensing policies and CA practices for e-commerce. Similarly, the South African Communications Security Agency (SACSA) could be authorised to establish or assist with the implementation of a licensing policy.

Questions for policy consideration

If South Africa intends to move forward with establishment of certification and public key infrastructure policies, there are several options and questions that will need to be addressed, among them:

- What architecture should a South African PKI have? The Task Group has recommended establishment of a Root (level 0) Government Certification Authority, which would certify the public keys of level 1 CAs in individual government departments. The Root Government CA might cross-certify root CA's in private industry sectors.
- Should legislation be passed to require mandatory, or at least voluntary, licensing of industry CAs? What structure should the licensing regime take? Which agencies should be responsible for establishing policy (the role of the *policy approval authority*) and for managing and implementing the licensing (the role of the *policy management authority*)?
- What should be the obligations and responsibilities, and the potential liability, of publicly licensed CAs with regard to electronic transactions, digital signatures, and cryptography? Should the UN and EU standards apply to the makeup and operations of licensed CAs?
- What organisations can be licensed to be CAs? Will unlicensed CAs be allowed to offer services? What distinctions need to be made between certification authorities and other forms of trusted third parties?
- To what extent should South African policy draw on and be reconciled with emerging international standards for certification and the potential for multiple competing certification authorities and certification procedures, applying to transactions across international boundaries?

4.5 Consumer protection and cyberfraud

If the measures discussed above for building trust in the integrity and security of electronic transactions are effectively implemented, these will go a long way toward ensuring that the digital environment is a safe and reliable medium for consumer purchases and other activities. However, there is still a long list of real and potential threats to consumer welfare in the emerging realm of e-commerce, and more are likely to appear in the future.

In brief, where there is commerce, there will always be those who seek to defraud the unsuspecting, or otherwise to misuse the technologies of the market for unwarranted or illegal gain. In the case of e-commerce, these technologies can be used in quite sophisticated ways, and there have already been many examples of very damaging and disturbing scams and abuse on the Internet. These can include false investment promises, so-called "spam" (e-mail advertising that jams mailboxes and servers), various pyramid and get-rich-quick schemes, or merely the problem of goods and services not being delivered as agreed. Other problems that have been previously discussed, such as the security of financial transactions and the protection of privacy, also fall into the province of consumer protection.

Lacking an established tradition of standard consumer protection laws or enforcement agencies even in conventional commerce, South Africa faces a difficult job of establishing such rules with respect to this new technological environment. It is utterly impracticable to police all communication that travels over the Internet, even within a relatively small community. To the

extent that law enforcement authorities lack the technical skills or resources to investigate illicit on-line activities, this problem is magnified.

Consumer protection in e-commerce includes an element of law enforcement in that laws dealing with fraudulent conduct in conventional commerce should apply equally to the digital environment. However, it would seem as if many of these laws are shrouded in language and "search and seizure" provisions that may be incapable of extending to the digital environment. Moreover, they generally apply only to South African territory; their jurisdiction does not extend to offenders residing outside our national borders.

Another aspect of consumer protection involves the question of liability of on-line intermediaries, webmasters, content providers and proprietors of websites, networks and servers, for fraudulent, illegal, or abusive transmissions or actions conducted over their servers, websites and electronic networks. Internet service providers (ISPs), for example, enter into service contracts with both end users and on-line merchants, and make at least minimal assurances for the quality and cost of these connectivity services. However, they seldom have direct responsibility for, or even knowledge of, the specific content of the websites that may be hosted on their facilities. Website owners and authors often merely retransmit information and commercial promotions that originate elsewhere. Laws that address liability for improper or fraudulent business practices in this environment need to be clear about the role of each participant along the chain of on-line services and transactions.

Current policy and initiatives in South Africa

As discussed in the previous sections, investigations into legislative and policy initiatives concerning consumer protection in the digital environment, data security, privacy and the like, are just beginning in South Africa. Some current consumer protection legislation and law enforcement issues may need to be revisited to ensure that a consumer or contracting party may enjoy at least the same measure of protection he or she would have enjoyed in conventional commerce. As stated earlier, a number of statutes have been identified which may present difficulties when applied to the digital environment. Apart from jurisdictional concerns, these statutes contain language and/or provisions that may be incapable of application to the digital environment. The Law Commission should comprehensively investigate the need for new legislation on many of these issues, and the South African Consumer Council may have a role to play. South Africa's participation in the WTO and other international treaties should also help to establish the parameters of policies that should be adopted, as these global agreements aim to harmonise practices across jurisdictions.

With respect to existing laws, according to the Edward Nathan & Friedland (ENF) report [4], the *Merchandise Marks Act of 1941*, the *Sale and Service Matters Act of 1968*, and the *Trade Practices Act of 1976* all contain consumer protection provisions designed to prevent fraudulent business practices. These protections could reasonably be interpreted to include deceptive advertising and schemes on the Internet, although they are generally limited to advertising about physical goods rather than virtual services. Investigation and enforcement of such on-line violations are not contemplated by the Act, which may need to be updated to incorporate cyberfraud concerns.

On the question of liability, the *Import and Export Control Act of 1963* as well as the *Sale and Service Matters Act of 1968* are unclear as to whether Internet service providers (ISPs) or other

on-line companies would be classified as intermediaries under their provisions. Clarification of these and similar definitions is important for enforcement and legal liability purposes.

Questions for policy consideration

- What new or amended consumer protection laws and regulations need to be established or adapted to reinforce the rights of the public in the context of e-commerce?
- 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?
- Should consumer protection and law enforcement issues form part of the subject matter of this Discussion Paper, or should they be addressed by their respective ministries and government departments, from time to time?
- What types of international agreement should South Africa pursue to ensure that cyberfraud and similar practices can be policed on a worldwide basis, through co-operative investigation and prosecution?
- What role should other consumer protection bodies (for example the Consumer Council) play in this regard?
- Should South African laws be established independently, or should the initiative come from international treaties?
- Should the issue of cybercrime be dealt with at the same time as general e-commerce legislation, or should the latter be dealt with first in order to hasten the process (as was decided during the UK e-commerce initiative)?

5. Establishing Ground Rules

In principle, users of e-commerce should expect to follow the existing laws, rules, and regulations devised for non-e-commerce. The perceived need for new rules to deal with unprecedented types of relationships and transactions does not mean that the old rules are irrelevant or need to be abolished. In fact, one of the stronger sentiments concerning the ground rules for e-commerce is that perhaps there *should not* be major new policies to apply to on-line transactions, such as "bit taxes" or new import duties on data transmissions.

Nevertheless, just as technology is changing consumer and business relationships, it is changing the nature of governments' oversight of and intervention in those relationships. The most profound manifestation of this change is in the globalisation of commerce, which places national governments and international institutions in a quandary as to which jurisdiction, and hence which set of rules, should be applied to which activities and by whom. The success of global e-commerce thus depends heavily on a worldwide harmonisation of certain basic policies in areas such as taxation and duties, as well as treatment of intellectual property rights and other trans-jurisdictional concerns.

5.1 Taxation and duties

Questions of taxation of electronic transactions, and of import duties on such transactions when they cross international boundaries, may be the most difficult and potentially troubling issues that governments must confront as e-commerce grows.

Tax issues take several forms. First, there is the question of "bit taxes": specific new taxes that might be applied to digital transmissions, separate from ordinary taxes that might already exist for products or services that happen to be purchased electronically. Many countries, such as the US, have adopted a total moratorium on any new domestic taxes on electronic transmissions in order to encourage the fastest possible development of this new form of business. Some countries, however, may find it difficult to resist an apparent new source of public revenues, or the perceived need to replace tax revenues that could be lost as commerce shifts to the electronic environment.

Far more complicated are issues of jurisdiction and institutional roles relating to tax collection under e-commerce. Operating in cyberspace implies that the physical location of a business is almost irrelevant, and possibly undetectable, as data files and related hardware can be easily moved from one location to another. This means that tax laws based upon the seller's "place of business" can become increasingly difficult to enforce, and countries with more lenient laws can quickly become tax havens for many types of businesses. It may be necessary to consider new types of taxation as well as new ways of monitoring and reporting business transactions, and greater international co-ordination of tax policies may be required.

Similarly, import duties and tariffs that differ significantly from one country to the next can create significant incentives or disincentives for companies to locate their virtual business operations in a given country. Governments wanting to foster greater international trade by means of e-commerce may be inclined to minimise duties on cross-border data flows and efforts to identify foreign information-based business transactions. Others may see a risk of erosion in existing public revenue streams by a shift of business activity toward on-line technologies. Again,

harmonisation of practices in these areas across jurisdictions will help foster a more equitable trade regime.

The WTO has taken a leading interest in e-commerce issues, particularly as they affect global trade policies. In their *Ministerial Declaration on Global E-commerce* in May 1998, the WTO Ministers order the General Council to establish a comprehensive work programme to examine these issues, with particular emphasis on the development needs of developing countries. As this programme goes forward, the Ministers agreed to continue a policy in member countries of "not imposing customs duties on electronic transmissions".

Current policy and initiatives in South Africa

There are no specific provisions in present legal texts that cover the treatment of electronically transmitted “goods” and services. Specifically, *the Customs and Excise Act 91 of 1964* defines “goods” to include all “*wares, articles, merchandise, animals, currency, matter or things”*, and it is unclear if this definition can be properly interpreted to include digital messages, software, multimedia files, even film and audio recordings. This uncertainty applies to the language in a variety of other laws, as well.

In addition, most other provisions of the customs law concern the physical delivery of goods, which must enter the country through some designated port at which customs officers can collect the duty and certify the import, using standardised paper documentation. These concepts do not address the reality of on-line services delivered to a user's computer terminal, over a communications infrastructure, without any opportunity for customs inspection, certification or duty collection.

The law further establishes definitions of the source or location at which goods, or parts of goods, are produced, for purposes of identifying domestic manufactured content. These provisions may be especially difficult to apply to digital goods that can be produced simultaneously in different locations, and copied instantly, without regard to jurisdiction.

These observations generally point out the degree to which tax and tariff policies in South Africa, as elsewhere, have not yet been able to be updated to encompass the realities of e-commerce. Although the Ministry of Finance has begun examining questions surrounding taxation issues, and the Ministry of Trade and Industry has been actively involved at the WTO in monitoring questions on trade and duties, there remains a relative void in policy and legislation. On the one hand, this situation could favour the development of e-commerce, if new taxes and tariffs are not applied. On the other hand, there could be problems if uncertainties about present or future tax and duty policy inhibit companies from making aggressive investments in new electronic business ventures.

Questions for policy consideration

- Should questions on taxation and duties form part of Government's current electronic commerce initiative?
- Should Government consider placing a limited moratorium on the levying of tariffs and duties on electronic commerce transactions?
- What changes need to be introduced to existing South African tax and duty laws to clarify their application to digital transmissions?
- To what extent should the government consider applying new or modified domestic taxes (income, value added) to e-commerce activities? What are the present and long-term revenue impacts of the shift toward electronically delivered services, payments, and revenues?
- How can on-line business activity be properly monitored and measured to comply with appropriate tax and duty obligations? What technologies and reporting techniques need to be employed?
- What positions should South Africa recommend to the WTO and similar international bodies on long-term policies regarding trade in digitally-based products and services? How do South Africa's interests differ from those of, for example, OECD countries?
- How should South Africa deal with the changing incentives for business location resulting from differential tax and duty treatment? What participation should South Africa have in international deliberations on the subject?
- What would be the optimum balance between regulatory and incentivised approaches to all the above questions?

5.2 Intellectual property rights and domain names

The future development of e-commerce rests heavily on two major intellectual property rights (IPR) issues, namely –

- the protection of copyrights and related rights; and
- the protection and equitable allocation of trademarks and domain names.

These concerns have been a primary focus of international deliberations in recent years, for example through the WTO, which has negotiated an Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), making intellectual property an integral part of the multilateral trading system since 1 January 1995.

Because so much of the consumer and business trade that occurs over the Internet involves selling or licensing of information, cultural products and technology protected by holders of intellectual property rights, this medium is especially susceptible to risks of theft or misuse of protected works. The TRIPS Agreement covers copyright and related rights (of performers, producers of sound recordings and broadcasting organisations), trademarks including service marks, geographical indicators, industrial designs, layout designs of integrated circuits, and undisclosed information such as trade secrets and test data. It aims to ensure the adequate

protection and effective enforcement of intellectual property rights and the impartial resolution of disputes between WTO members.

Both the TRIPS Agreement and the copyright treaties of the World Intellectual Property Organisation (WIPO) recognise that copyright protection covers compilations of data or other material the contents of which constitute intellectual creations. It has been informally agreed that the impact of digital technology on copyright and related rights has to a large extent been to enable production and distribution of pirated sound recordings, films, software, CD-ROMs, etc. Despite the legal protections offered by these international agreements, the use of trademarks on the Internet continues to raise important questions, for example with regard to jurisdictional authority.

This can be important for South Africa in at least two ways. First, South Africa's membership and participation in the WTO and WIPO make it vital for the country's laws to be in conformance with those treaties, and for law enforcement and customs authorities to help enforce intellectual property right protections, to ensure uninhibited fair trade. Second, the interests of South African creators of intellectual products, including software, recordings, and technical designs, need to be protected both domestically and internationally from illegal pirating of their works and from unfair use of South African trademarks.

The relationship between trademarks and Internet domain names is also receiving considerable attention. Under each top-level domain (.com, .org, .net, etc.), second-level domain names have to be unique (at least within each country) and have typically been allocated on a first-come, first-served basis within each top-level domain. Trademarks, however, may co-exist in different categories of products and services, and in different territories (see also further discussion in Section 6.3 below).

Another controversial question concerns the use of a domain name that is identical or similar to a trademark: under which jurisdiction(s) would it constitute a trademark infringement, and what remedies should be available for the trademark holder? It is not clear how best to develop the governance of the domain name system, and there is a pressing need for a widely acceptable resolution. Conflicts over principles exist between the US and several other countries. This issue may have added significance for developing countries such as South Africa if the domain naming system, by default, tends to favour websites in the US, where the system originated and the majority of sites are still hosted.

The Internet Corporation for Assigned Names and Numbers (ICANN), recently established in the US but under the wing of the Internet Society, will aim to appropriately administer policy for the development of competition in Internet names and addresses. There is resistance to a US-based initiative because a number of countries are seeking to adopt their own domain name systems. Such a view is expressed in a resolution adopted by the ITU (International Telecommunication Union) Plenipotentiary Conference, which stressed “the need for the future system of registration, allocation and governance of Internet domain names to equitably balance the interests of all stakeholders, in particular businesses and consumers, and not to privilege any country or region of the world to the detriment of others”. ICANN is currently developing its mandate and looking to appoint non-US directors to ensure international buy-in, but there is still some debate as to the exact way in which various countries might respond to this development.

Current policy and initiatives in South Africa

According to the Edward Nathan & Friedland report, there are several laws currently on the books in South Africa concerning trademarks, copyright and similar intellectual property issues that may need to be updated in the light of e-commerce. For example, the *Merchandise Marks Act of 1941* is primarily aimed at preventing fraudulent marketing of products or goods, and does not apply to services. To the extent that software and other media sold over the Internet are generally classified as services, the law's provisions would not apply, and there is no other established legal precedent to ensure protection of companies' trademarks in the virtual environment in South Africa.

The recent *Counterfeit Goods Act of 1997* goes somewhat further but retains some ambiguities. The purpose of this Act is to prevent the sale and possession of counterfeit goods, but again this does not clearly extend to virtual goods such as software and multimedia transmissions. The Act does define "documents" to include magnetic media and other electronic forms, but this is principally in relation to evidence of counterfeiting, rather than to actual goods that could be considered counterfeit.

There may be similar questions concerning the *Business Names Act of 1960*, the *Trade Marks Act of 1993*, and the *Copyright Act of 1978*. In January 1998, the legislature did pass the *Intellectual Property Laws Amendments Act*, which sought to revise and update some of these and other laws dealing with intellectual property rights in South Africa. This was done in part to bring the country more into line with the TRIPS Agreement and the Patent Co-operation Treaty. One important set of amendments affecting e-commerce involved the *Copyright Act* and the treatment of copyright in computer programs. Specifically, the amendments apply copyright protection to the reproduction, publishing, broadcasting or transmitting of computer programs in any manner, and any adaptation or use of such programs. These changes should be further reviewed in light of the other distinctions in current law mentioned above, but they appear to set a precedent for preventing improper use of intellectual property in the digital environment.

South Africa has been an active participant in international deliberations on intellectual property rights issues before the WTO and the WIPO. South Africa also hosted a regional consultation of the WIPO in October 1998, with participation by the Patent and Trademark Office among others, along with representatives of several other African countries. The consultation focused on the domain name issue, with an emphasis on understanding the concerns of developing countries in this area.

Questions for policy consideration

- In present and potential South African law, what activities in a digital, virtual environment should constitute an infringement on a registered trademark or copyright? If the use is considered to constitute an infringement under South African law, what remedies should be available, in particular if the transmission originates in another country? What specific legislative changes should be considered?
- Are the recent amendments to the national intellectual property laws sufficient to comply with international treaties and the demands of e-commerce? What further amendments and improvements should be considered?

- Are the provisions of the TRIPS and WIPO treaties adequate to protect and promote the interests of South African intellectual property rights holders? How in particular does this prevent the exploitation of indigenous knowledge? What should be South Africa's position on further participation in and revisions to these treaties?
- What are the particular concerns of South Africa with respect to domain names? Should a domestic domain name policy and authority be established? (See also Section 6.3.) How can the brand names of South African companies and products be protected in an international environment, particularly in the establishment of a new domain name system?

6. Enhancing Infrastructure

Electronic commerce is entirely a phenomenon of the technological revolutions of the late 20th century: in computers and information systems, in telecommunications, and also in banking systems and even postal and delivery services. It is the advancement and the integration of the essential infrastructure of these technologies that has fuelled e-commerce growth worldwide. At the same time, the comparative lack of such infrastructure throughout many parts of the developing world is what most impedes the opportunities for e-commerce to flourish in those countries, and to accelerate their economic and social development.

In South Africa, access to infrastructure is not equitable. In Johannesburg, Cape Town, Pretoria, and other urban centres, high technology facilities and services are widely available to those portions of the population who can afford them. However, for vast segments of the population, in rural areas as well as in townships, available infrastructure is often meagre at best, and typically unaffordable as well. Accordingly, the need to enhance the national infrastructure to support e-commerce is one of the paramount concerns for South Africa. With the low level of basic telephone service penetration in rural areas, and access to computers and data services even lower, the possibility of participating in the global electronic marketplace is remote for much of the country's population. The same is true of access to banking and financial services, which are equally necessary if consumers and small businesses are to conduct commerce in a digital environment.

Because of the critical nature of these issues, both government and the business community in South Africa have begun to take initiatives to expand and upgrade existing infrastructure, to provide more equitable access to needed services and technologies, and also to increase the size of the national marketplace. More progress is needed, however, and many questions remain concerning the direction of policy in these areas in the near future. The topics discussed below thus focus on the main issues and options confronting South African business and government leaders in their efforts to close the infrastructure equity gap and to bring the opportunities of e-commerce to the entire population.

6.1 Information and communications technology (ICT) infrastructure

Access to ICTs is the most basic prerequisite for e-commerce. In the developed world, telecommunications infrastructure and computer facilities are widely available (albeit not universally), at costs that are within reach of the majority of the population. In South Africa, by contrast, as in other developing countries, these facilities are accessible only to a privileged minority, and many small and medium-sized businesses remain unconnected, especially to advanced technologies.

There is general agreement about the desirability of expanding access to computer and communications technologies, but there are major questions about the most effective means to achieve this goal. Traditionally, for example, telephone services have been provided by state-owned monopoly utilities (Telkom in the case of South Africa), which have pursued principles of "universal service" through policies of cross-subsidy and market exclusivity. As technological and economic conditions have changed, however, international policies have focused increasingly on

a transformation to private, open market options to promote investment, efficiency, and innovation in telecommunications.

The dramatic changes represented by e-commerce may be changing the economics of telecommunications and information access, even for relatively remote rural and lower income populations, as incentives to connect these users to the global marketplace increase. Meanwhile, the definition of "basic" telecommunications service itself has come into question: basic service used to mean traditional two-way voice telephony, but this type of service may be less essential in a networked world than access to data transmission, the Internet, electronic mail, and the like. Governments also see the value of information technologies as efficient means to deliver public services, such as education and health care, to the broader population.

Developing as well as developed countries seeking to take full advantage of these technologies are looking into the establishment of Multipurpose Community Centres (MPCCs). These offer a combination of telecommunications and information services to the general public at affordable prices. The idea of MPCCs is to promote universal access to technologies that would be unaffordable and unavailable to most citizens and even many businesses, beyond the higher income and most developed urban regions. The policy of encouraging MPCCs also seeks to support local economic development, integrated public and private services, and broad education and training, in addition to the traditional goals of communication, information, and inclusion in the national economy.

Current policy and initiatives in South Africa

Some of the most important policy initiatives to transform the South African telecommunications infrastructure were established with the passage of the *Telecommunications Act of 1996*, and the negotiation of a strategic international partnership between Telkom and Southern Bell Corporation (SBC) and Telekom Malaysia. A principal requirement of the new license for Telkom is the rollout of an additional 2.8 million telephone access lines throughout the country over five years (combined with exclusive control of the basic service market during that time). This programme, which has been progressing rapidly for more than two years now, will bring new services to a large number of customers in unserved areas. However, it is not sufficient, by itself, to achieve all of the infrastructure needs for e-commerce.

The Department of Communications has begun a strong series of policy actions to promote more widespread access to communications and information technology in South Africa. The Department's broad set of programmes, grouped under the banner of the "Info.Com 2025" initiative, encompasses nearly every aspect of ICT infrastructure and applications, with ambitious goals of bringing South Africa into the forefront of Africa and the developing world and on par with international standards in technology development and infrastructure deployment [5].

One of the centrepieces of South African policy has been the establishment of the Universal Service Agency (USA) to develop a network of telecentres throughout the country, and the associated Universal Service Fund (USF), to which Telkom and the cellular operators contribute. This project is moving toward a vision of something close to universal ICT access for all South Africans in the foreseeable future. The project has been in the initial experimental and planning stages; more widespread rollout of a range of micro, small, medium, and large telecentres is to commence in the coming months.

One of the most critical unresolved policy questions for South Africa is the future market structure of the telecommunications industry following the termination of Telkom's exclusive franchise over most basic and enhanced services after 2001-2002. There is a general expectation that the market will be opened to new participants, but beyond that, the shape of competition remains fairly open. The ultimate decisions in this area will have an important impact on the scope of infrastructure development.

The challenge is to define incentives and obligations for new investors in the sector – both domestic and foreign – to provide basic and enhanced services to unserved areas, in a manner that will be both commercially viable and socially beneficial. This policy is also tied closely to the telecentre development initiative. If telecentre operations can help fuel community economic development, then the market for telecommunications access will expand commensurately. The telecentre operators themselves may be among the most eager candidates to enter the telephone service market, to gain some independence from Telkom and to expand their own business position. This might happen through the creation of community-based rural co-operative telephone companies, through a national consortium of telecentres forming a competing local and backbone network, or through an alliance with other entrepreneurs. In addition, the cellular operators, Eskom, Transtel and other potential players might be encouraged to support the telecentre programme as part of their market entry opportunity.

Many other questions will need to be addressed in the context of the market opening policy. These will include interconnection regulation, treatment of Universal Service Fund contributions, tariff regulation, cross-ownership with other industries, the role of ICT in government, and a number of other issues. DoC will collaborate with other government departments to deal with these questions in the context of its overall strategy for infrastructure development and the promotion of universal access to communications and information technology.

Questions for policy consideration

- What should be the priorities and objectives for telecommunications market development in South Africa?
- How should the goal of universal access be balanced with the need to maximise hi-tech development, global participation, and revenue opportunities for South African companies?
- What policies should apply to the opening of the telecommunications market to competition? How broad should market entry options be, who should be allowed to participate, under what conditions and in what service market segments? What restrictions should there be on foreign investment, cross-ownership and Telkom's position?
- How should universal service obligations be incorporated in the emerging market for new carriers? Should all entrants have equivalent obligations, or should new participants enjoy more leniency until they are better established? What should be the tradeoffs between construction obligations and payments to the USF?
- Should government encourage the formation of rural co-operatives or other local telephone franchise investments? How can this be accomplished, and what resources should be committed?

- What will be the process for determining interconnection obligations in the market? How can new carriers, especially small local operators, be assured that they will be able to interconnect affordably to the national network?
- How much emphasis should be placed on supporting domestic manufacture and employment in information technology sectors, compared with the goal of rapidly expanding available infrastructure?

6.2 Telecommunications market and pricing regulation

Even in countries where open competition in telecommunications has become relatively widespread, regulation of the industry remains an important public responsibility, both to support fair competition and to oversee appropriate pricing and service responsibilities in those market segments where competition is not fully developed. Such economic regulation is even more crucial in developing countries, as market forces are not likely to emerge strongly enough to constrain dominant operator actions in the near future. As mentioned above, this will become an increasingly important responsibility as the South African market is opened to competition.

The prices charged by telecommunications operators for access to crucial services can be a major factor determining the effectiveness and affordability of e-commerce opportunities on the whole. These services include high-speed data transmission links between local companies and the Internet backbone (typically via international circuits), as well as end-user connections to internet service providers (ISPs) and other data and information services.

Traditional pricing policies, for example, have led to charges for high-end data links in many developing countries that are vastly greater than similar charges in places like the US, making it extremely burdensome for smaller entrepreneurs, ISPs, and public operations such as telecentres to afford to connect to the global backbone. It may be appropriate to re-examine these pricing policies, ideally in the context of an overall review and revision of the market structure for telecommunications in general, with the understanding that the costs of data communications, even when provided to large businesses, will inevitably be passed on to end users and can form a barrier to e-commerce development.

Current policy and initiatives in South Africa

Telecommunications regulation in South Africa is principally the responsibility of the South African Telecommunications Regulatory Authority (SATRA), under the mandate of the *Telecommunications Act of 1996*. SATRA began operations in 1997 and has already taken a number of important initiatives to promote development and access to traditional and new communications services. Among its earliest and most highly publicised decisions was to classify internet service provider services as "value-added", and hence not within the exclusive control of Telkom (see next section).

SATRA's other major initiative recently has been to manage the process of issuing a third national cellular telephone service license, which should be completed later in 1999, further expanding the market for mobile services, and increasing competition. SATRA has also been actively involved in the development and implementation of universal access policy together with the Universal Service Agency, and has conducted a variety of studies and policy reviews on important industry issues such as frequency assignments, interconnection, call-back and Global Mobile Personal Communications by Satellite (GMPCS).

SATRA has not, however, had much specific authority regarding regulation of Telkom's services and prices. To the extent that Telkom is able to set its prices for data services and other essential elements of e-commerce without regulatory oversight, this could create economic barriers, especially for the most disadvantaged users. One option could be to authorise SATRA to influence prices for services provided to community telecentres, to ensure that these operations can offer services to the public on the most cost-effective basis.

Questions for policy consideration

- Is the current structure of telecommunications regulation adequate to support robust infrastructure and service development in South Africa?
- How should pricing policies for data and Internet-oriented telecommunications services be revised? Does SATRA require additional authority and flexibility to investigate Telkom's services and price?
- Should multilateral policies be revised to alter the current pricing and service arrangements for international data circuits and for connecting national networks to the Internet backbone? How can South Africa participate in such negotiations?

6.3 Internet services, governance and domain names

The Internet has become the central engine of global e-commerce. Communication, marketing and transactions are all carried on worldwide via this interlinked network of networks, which can potentially be accessed by anyone with a telephone line, a computer and an internet service provider (ISP). The “ISP infrastructure” is closely related to the infrastructure of telecommunications and computer facilities, and is essential to the prospects for e-commerce. The Internet itself is at its core an unregulated, almost anarchic system that grew up without any formal government or even industry policy to guide it, evolving as a result of hundreds of unconnected technical experiments and *ad hoc* standards and protocols. Arguably, the success of the Internet is largely attributable to this lack of regulation, which has allowed the creativity of programmers and entrepreneurs to flourish.

The expanding scope and importance of Internet communication has, however, led to a situation where it is hardly possible to avoid some form of governance of its organisation and operations. An example of such governance is the Internet Co-operation for Assigned Names and Numbers (ICANN) that was established recently. This applies especially to the Domain Name System (DNS), which assigns domain names to individual (and corporate) website hosts, but there have also been policy discussions concerning potential regulation of the technical and business aspects of internet service provider (ISP) services, and also of the content of Internet-based communications. South Africa also has to confront these questions and determine what policies, if any, it wishes to pursue with regard to regulation of Internet services.

Access to ISPs

In their most basic form and function, ISPs are not telecommunications operators, and they need not directly supply any communications transmissions facilities, either to themselves or to their customers. Rather, ISPs provide computer processing and storage facilities – routers and servers – that retrieve, store, convert, and forward electronic data. The connections between end users

and ISPs, and between ISPs and Internet backbone routers and servers, are provided by Telkom or by other telecommunications network operators, and services such as data and voice are essentially indistinguishable over the Internet protocol.

Access to ISPs is therefore just as important as access to basic telecommunications network facilities, if end users and small businesses are to be able to take advantage of Internet-based e-commerce opportunities. In some countries, ISPs have to be licensed by government authorities, or only the monopoly public telephone operator is allowed to provide these services. This can lead to slow development of the market and high prices to the public, but it may allow the government a degree of control over the provision of services and content (see below). The South African experience to date, similar to that in the US and most of Europe, has seen the rapid growth of dozens of local, private ISPs, and consequently a wide availability of these services at competitive prices throughout the country.

Nevertheless, the problem of access to ISP services in the most rural areas has yet to be fully addressed. As Telkom's rollout of new lines and the Universal Service Agency's telecentre programme expand the availability of basic telephone connections into rural communities, the full objectives of universal access to information and communications technologies will not be met unless these services include full-featured access to the Internet as well. This implies higher capacity, digital data connections, as discussed above, but it also demands that the services of national ISPs be expanded and new, local ISPs be established to serve the needs of e-commerce entrepreneurs and consumers alike. The Universal Service Agency's telecentre development plan includes some provisions for promoting development of such ISPs, and there may be other means for integrating ISP and basic communication access for rural subscribers.

Domain name regulation

As mentioned in Section 5.2 above, treatment of domain names has become an international policy issue involving treaties on intellectual property rights. Beyond the questions of protecting trademark holders, there is a basic need for an organised process for assigning domain names within the South Africa country-level domain (**.za**). This will be increasingly important as e-commerce expands and domestic companies establish Internet-based marketing and services that will be associated in the public mind with their brand name, and hence with their on-line domain name. To date, registration of South African domain names has been undertaken by private companies through the international DNS registration system, with no national mechanism for applying for domain names or verifying the validity of an applicant's use of a particular identity.

Current policy and initiatives in South Africa

The Internet has been accessible in South Africa since the early 1990s. Since 1994, commercial use of the Internet has been driven by a small group of private sector ISPs that purchase capacity from Telkom and sell Internet access services to individual and corporate customers. Growth in this sector has been quite rapid: by 1996 there were estimated to be as many as 60,000 South African websites and over 250,000 Internet users, growing to over 600,000 Internet users by 1998. There are now some 72 ISPs in South Africa, and the ITU has ranked the country 18th worldwide in terms of the number of Internet host computers.

Despite the strong Internet usage and growth, especially for a developing country, access to the Internet remains highly restricted to particular geographic locations and segments of the

population, due to historical inequities in the society and economy, and the lack of access to basic telephone service and computers, particularly in rural areas. For these reasons, the Department of Communications has focused on the expansion of Internet access as one of its most fundamental policies, instituting projects such as Public Information Terminals (PITs) and Internet-2000. As mentioned, the Universal Service Agency is also emphasising availability of Internet access in its telecentre implementation plan.

Nobody currently bears specific responsibility for the regulation or governance of Internet services in South Africa. SATRA has taken a strong position against Telkom's claim that its exclusive telephone service franchise should also extend to ISP services, and while that ruling is undergoing a court challenge, the independent ISP industry has been thriving in an unregulated environment. There has been discussion about establishing some form of new governance structure. In the public sector, the commercial WAN Service Provider (previously called GOVNET) has been responsible for managing the **.gov.za** servers for the government for several years and may, if required, extend its service to the private sector.

Questions for policy consideration

- Should SATRA's position on a competitive ISP industry be supported by legislative action or other policy?
- What means, technical and financial, should be employed to promote new ISP services in rural areas? How should these services be integrated with the telecentre plans and Universal Service Agency rollout plans?
- Should South Africa create formal governance structures such as a domain name registration authority? Who should take responsibility for these functions?
- Should there be any attempt to regulate the quality, availability, and pricing of ISP services (whether provided by Telkom or independent companies)?

6.4 Banking and financial services

The financial services sector cannot be overlooked as a critical element of the infrastructure necessary for e-commerce to succeed. Currently, transactions that occur electronically do not typically involve cash payments or any direct transfers of funds between buyer and seller. Instead, e-commerce transactions rely upon the intermediary role of banks, credit card companies and other financial institutions, which must therefore be thoroughly interconnected to the communications and data-processing web.

This requirement raises further challenges for most developing countries, although to a large extent South Africa's banking services and technology are reasonably on par with those of more advanced economies. The needed infrastructure extends in two directions:

- to link local and national businesses with global banking networks to allow for efficient domestic and international business-to-business transactions; and
- to give consumers, small businesses, and local communities access to financial resources and services that will allow them to participate effectively in e-commerce.

The first need, namely for sophisticated business-oriented financial services, demands the most up-to-date banking systems along with the general data-processing and communications

technologies required for on-line connectivity. For domestic businesses to compete in the global market, they must be able to effect seamless, reliable transactions with a minimum of faults, delay, complication and cost. The development and maintenance of this infrastructure should be in the interest of the banks themselves, as it improves the quality and efficiency of the services provided to their customers.

The banking infrastructure needed at the local, consumer side of e-commerce may be considerably more difficult to achieve. Just as the majority of South Africans do not have access to sophisticated telecommunications services, a large segment of the population also lacks access to even basic banking services: savings and cheque accounts, credit cards and loans, even simple cash currency in some cases. It will require creative and co-operative efforts on the part of banks, Government, businesses and community leaders to develop innovative means of reaching these unserved groups with services that are both appropriate and affordable.

Infrastructure for electronic payments

Another important issue in this area is the general technical question of electronic payment systems. Again, these issues relate to both business- and consumer-oriented transactions. For businesses, there are several mechanisms that have been well established for many years, such as electronic funds transfer (EFT), financial electronic data interchange (FEDI) and international Society for Worldwide Interbank Financial Telecommunications (SWIFT) payments. These facilities are becoming more widely available and easier to use as many banks have introduced on-line account access and the opportunity for customers to effect transactions remotely over the Internet.

For consumers, electronic payments can readily be made using traditional credit and debit cards and new types of credit instruments that are being introduced. Questions surrounding the security of these forms of payment are among the key concerns involved in building trust in Internet-based transactions (see above). Even if these mechanisms can be made secure and effective from the consumer’s perspective, however, they may not always be the most efficient ways of transferring funds around the world over the Internet. Other alternatives being considered within the industry include so-called “digital cash” (also referred to as “electronic money”) and prepaid accounts. Some of these ideas might also be applied directly to the challenge of serving customers who lack access to full banking services.

In summary, most digital cash proposals involve the establishment of a virtual bank account into which the user deposits some amount of funds, or through which he or she establishes a line of credit. The account operator (which could be a bank, credit card company, or retailer) establishes relationships with on-line merchants that allow for payments to be made directly from the subscriber's virtual account for purchases from those merchants. When selecting a product for purchase, the user may authorise payment by means of a secure, coded transmission, similar to a digital signature. This instructs the account operator to effect a transfer of funds from the user's account to the merchant (including a transaction processing fee to the intermediary). Although this system exists in various forms, particularly for certain well-established on-line merchants, there is no single standard or worldwide coalition of providers. Issues of security and trust, and also of competing interests by the financial and retail firms involved, have slowed acceptance of these types of services to date, but they are likely to continue to gain acceptance in the future.

Another mechanism that has been gaining popularity with companies and consumers is integrated circuit cards, commonly known as "smart cards". Smart cards contain programmable microchips which can be set to identify the total value of the card (in the case of "pre-paid" cards), or the amount of funds on deposit in the user's associated bank or virtual cash account. The cards can be issued by a specific merchant or service provider (telephone smart cards are especially popular), or can serve as general purpose payment vehicles. The cards can be used to make regular transactions, with the amount of the payment deducted automatically (by a cash register, public telephone, or other machine) from the total available on the card. Some smart cards allow the user to replenish their value by making new payments or deposits to an authorised agent who has the technology to update the card's chip to the new amount.

Smart cards or similar ideas might be especially useful for providing financial services and access to electronic payment systems for the so-called “unbanked”: consumers in rural areas or others without access to bank accounts and credit cards. Instead of paper pay cheques, for example, the general public could receive payment for their jobs or transfer payments via electronic transfers, by adding the correct amount to their personal smart card. The benefits could include reduced risk of theft and fraud, and much wider access for the general public to both electronic and traditional products and services.

Current policy and initiatives in South Africa

South Africa's financial services sector is well advanced, especially for providing business services in the urban areas. The South African Multiple Option Settlement (SAMOS) System was developed by the South African Reserve Bank and has been operational since 1998. This system links all the settlement banks in the country and allows real-time settlement between the banks. Major South African banks have data networks connecting their branches and large corporate customers, and have been promoting the use of EFT, FEDI and automated teller machines (ATMs). Some banks are also launching smart card initiatives.

These accomplishments mean that the South African financial sector is well positioned, especially with regard to large corporate businesses, to support widespread applications of e-commerce. Indeed, South Africa can be a leader in e-commerce throughout Africa, offering such financial services and other support to other countries in the region.

There are real opportunities for expansion of these initiatives to the rural and disadvantaged communities of South Africa. Despite the strengths that are in place, large segments of the population remain without access to banking services. Just as physical infrastructure must be made available, creative programmes for providing access to these advanced banking and credit technologies must also be emphasised by both government and the financial sector.

The South African Reserve Bank has published a position paper [6] on "Electronic Money", in which it discusses traditional and new options for making electronic payments, including digital cash and smart cards, and the authentication and technical implementation issues surrounding them.

Questions for policy consideration

- What steps need to be taken to further upgrade and integrate national financial services infrastructure to facilitate e-commerce?

- How can basic banking services be extended to the broader population, to allow use of electronic payments, credit, and funds transfers?
- What types of electronic payment systems and technology are most appropriate and practical? How can these be developed effectively on a national level, in co-ordination with international industry efforts?
- How should the government support these development efforts, both logistically and financially? Which agencies should be responsible? Are there legislative actions that need to be considered?

7. Maximising Benefits

For a country such as South Africa, one of the most important benefits of e-commerce is its potential to help a developing society to leapfrog into the knowledge paradigm (refer to Section I, Introduction). The positive effects of e-commerce can be magnified beyond purely commercial growth to have a profound impact on all aspects of society. Most of the policy debates and proposals surrounding e-commerce are geared toward removing barriers and promoting opportunities for these new types of commercial activity to expand even more rapidly than they already are. In light of the potential impact of e-commerce on our society, a final category of issues can be seen as focusing more directly on the benefits to be gained from e-commerce, particularly the benefits that developing countries might achieve with successful strategies.

It is apparent that most of the major developments in this field have sprung from the private sector, and will continue to do so in the future. Government can, however, play an important role in examining the economic and social impact of e-commerce technologies and in promoting understanding and application of these technologies throughout South African industries and communities. Various government agencies, through co-ordinated policies and programmes in conjunction with private sector partners and institutions, can help maximise the benefits of e-commerce by –

- facilitating market access and business opportunities, especially for small, medium, and micro enterprises (SMMEs), on a national and global scale;
- providing educational and skills development resources;
- supporting the rapid deployment of necessary infrastructure (as discussed in the previous section);
- facilitating the development of MPCCs as vibrant seeding points for community knowledge and wealth creation, above and beyond the provision of the latest ICTs;
- developing “model use” programmes for the dissemination of government information and services using e-commerce platforms, e.g. for electronic tender processes;
- supporting necessary transitions in the labour force due to technological and industrial transformation; and
- ensuring equity in the availability of opportunities and benefits, in the context of the overall development of South African society.

The sections that follow present an overview discussion of the issues surrounding the impacts of e-commerce on society and the economy, along with some of the activities already taking place in South Africa to promote the benefits of these developments. Finally, suggestions and questions for further policy responses are presented for consideration by South African industry and government officials.

7.1 Economic and social impact of e-commerce

Electronic commerce, and information and communications technologies (ICTs) in general, are rapidly transforming many aspects of the basic social and economic structure of the world we live in, moving out of the industrial era and into the Information Age, forming what have been called a knowledge society. Business relationships are changing, becoming more global in nature, while at the same time many enterprises are decentralising and smaller businesses are playing a larger role in the economy. Socially, the status of the individual and the family are being affected in

ways still not entirely understood; we are becoming part of a global village, but may simultaneously be more isolated from those around us.

These fundamental trends in the economy and society can be both beneficial and detrimental, depending in part on how well they are understood and managed by the institutions – government, educational, corporate – that are most directly affected by the new socio-economic and technological paradigms. The challenges lie at two levels:

- The first challenge is to understand, and even anticipate, the currents of change and their many impacts, to recognise inevitable trends, and to predict the cumulative effect of the many separate but interwoven decisions in all spheres on the daily lives of citizens.
- The second is to respond to these trends positively, reinforcing their benefits and counteracting their detrimental aspects as effectively as possible, through co-ordinated policies and partnerships on a local, national and global scale.

Some of the basic impacts of emerging e-commerce and ICT developments that have been identified are summarised below:

Economic impacts

- The rapid pace of technological change and the global nature of markets have confronted governments and especially businesses with an "adapt or die" scenario. Particularly in developing countries, to fall behind in technology and innovation could increase the gap with wealthier, more advanced economies.
- Conversely, as mentioned in Section I, e-commerce presents unique opportunities for less developed countries to greatly expand their markets, both internally and externally. Externally, the Internet and other technologies may allow for low-cost international trade, even for small, local businesses. Internally, many groups of citizens who had been considered "marginalised" and "unbanked" may gain affordable access to financial services, and may thus participate more readily in all aspects of the economy.
- E-commerce technologies carry the potential to reshape the very structure of the national landscape. Central business districts may become less relevant, as companies and workers can conduct business with equal effectiveness from almost any location. Rural areas considered too costly or unprofitable for business development might increasingly become a focus for investment and market expansion, and also for relocating corporate offices.

Social impacts

- Some of the intangible downside risks of increasingly “virtual” interaction within society include the possible “desocialisation” of individuals who have less and less direct contact with their peers, their co-workers, their community. This can extend to family relations as well, particularly if technology creates further imbalances between those who are “on-line”, and those without access to these technologies. On the other hand, equitable deployment of infrastructure and educational resources could provide a means of maintaining and expanding family and communal ties that would otherwise be broken by distance and cost.
- Other possible problems, including psychological and physical health-related effects of sedentary, computer-anchored work environments, have not been fully examined. Early experience suggests that as this type of work (and social) activity expands, businesses and

government will have to consider broad-based means to offset health hazards with new policies and treatments.

- On the whole, e-commerce may offer the potential for shifting the balance of opportunity, wealth, and social and political inclusion. As much as these trends can be beneficial to the majority of society, they are also likely to bring unanticipated effects on cultural and social norms. Indigenous traditions that have so far survived the intrusion of modernity may be less resilient in the face of global networks and instantaneous communication. These types of impact are just as significant as changes in bottom-line incomes, and can really only be "measured" by the persons whose lives are being changed by forces largely beyond their control.

7.2 Development of market access and business opportunities

E-commerce is in its infancy, and as such requires special attention and perhaps even temporary policy measures to ensure that it is nurtured and allowed to develop its full potential. The exploitation of its potential to transform a developing economy can be measured in terms of factors such as the development of SMMEs and participation in the global economy.

Supporting SMMEs

Electronic commerce opportunities are valuable for giant corporations and small entrepreneurs alike. In the latter case, however, the technologies and market options available through e-commerce may foster a true revolution in the way business structures and relationships are organised. The prospect of establishing new small, medium, and micro enterprises (SMMEs) is greatly enhanced by the efficiencies available through information and communications technologies. These include access to global supply chains, the costs of marketing, obtaining vital input resources, conducting research and development, and all manner of financial transactions. In short, many business functions that previously depended upon large, integrated organisations – from record keeping to sales to training to administrative and secretarial work – are now increasingly "outsourced" to small or specialised companies or the self-employed. This arrangement offers flexibility and customised work arrangements to both clients and employees.

Most of these types of business opportunity require basic computer literacy such as word processing and Internet browsing skills. This implies that successful entrepreneurs will be those with some skills and training in these technologies, as well as an understanding of the basics of business management and finance. As discussed below, it will be in the interest of the government as well as the private sector to support accelerated education programmes in these areas, to facilitate the rapid growth of new small business development.

Ensuring global participation

Another revolutionary feature of Internet-based commerce is that it expands the size of any business's potential market from its immediate geographic locale to a potentially worldwide arena. This unparalleled expansion of market access and opportunities for existing and new businesses has created a potential for accelerating economic growth in developing countries, including relatively poor and rural areas. The process of discovering how to tap these global markets, and how countries, communities, and entrepreneurs can get more leverage for their

unique skills and knowledge, is only just beginning in most countries. In some cases, indigenous craftspeople have been able to sell their products to a global customer base. For others, increased tourism may be a strong opportunity. Where a workforce is skilled in ICTs, the Internet can often provide direct employment opportunities in software development, data processing and many other information-intensive jobs.

A global market demands world-class quality service as well as the flexibility to meet very differing needs. These requirements place a heavy responsibility on new electronic merchants to use state-of-the-art web design, interactive media, different language options and other features to ensure consistent user-friendliness and relevance to a diversity of clients. Newcomers to the digital market will find this degree of sophistication quite a challenge to achieve. There will consequently be a great need for business development support programmes and for training in e-commerce applications.

There is also a vital need for sharing of information and experience among web-based businesses, particularly those from developing countries that may discover market opportunities, strategic advantages, and unique approaches to this emerging industry which could be of value to their counterparts in other countries and other markets. New networks are springing up to connect Internet-based businesses for this type of intelligence sharing, and also for joint marketing initiatives. These activities are being sponsored on a global level – for example by the Global Trade Point Network of the United Nations Conference on Trade and Development (UNCTAD) – as well as by national Ministries of Trade and Tourism and by many private industry associations.

The opening of national boundaries for wider market participation works in both directions, so the benefits can be accompanied by risks to domestic markets and consumers. As discussed in the previous section, debates continue at the level of the WTO and other fora over the proper balance, especially in developing countries, between fully open trade markets and the need to protect national interests. These issues transcend e-commerce, but the ease and immediacy of cross-border trade via telecommunications compels governments to adopt a greater sense of urgency as they weigh the tradeoffs.

Foreign investment and international partnerships become easier to negotiate in an electronic environment, where foreign partners may never need to set foot in the country where they invest. The challenge in such relationships is for domestic partners to secure not only short-term capital but also lasting benefits such as technology transfer, training and reciprocal market access. Similarly, risks associated with unrestrained markets – such as the dumping of sub-standard products – may be accentuated in the e-commerce environment and need to be carefully monitored.

7.3 Impact on the workforce

The labour market is one of the areas likely to feel the most profound impact of the economic transformation being brought about by e-commerce. The scope and magnitude of that impact is an open question, subject to debate along many dimensions. On the one hand, if e-commerce generates significant economic growth in general, this should lead to improved employment opportunities across the board. However, the exact nature of employment, and of the skills and experience required to benefit directly from e-commerce, could be significantly different in some

industries from the traditional employment mix, meaning that many workers could become displaced, temporarily or permanently, as a direct result of this transformation.

Specifically, as detailed in the introduction, the shift from an industrial paradigm to a knowledge paradigm implies that the central base of much economic activity is shifting from industrial production to a knowledge economy. These changes are likely to lead to the elimination, or at least transformation, of many traditional job functions and even entire companies. This presents a short-term risk to workers whose current jobs and skills are concentrated in obsolescent industry segments.

The counterpoint to this concern is that there should be considerable long-term opportunities, both for displaced workers and for the unemployed and younger, new graduates. Given appropriate support for retraining and hi-tech education, these workers can find a wide range of job openings in new and expanding industries.

In a more fundamental sense, the shift away from manufacturing and heavy industry may imply a transformation of the very concept of a “job”. In an information economy/knowledge society with rapidly changing technologies, services, and markets, individual workers' skills are likely to be more transferable across companies and job descriptions, and this flexibility could be of benefit to both employers and workers. The phenomenon of "permanent temporary" workers or individual contractors could supplant traditional relationships between employer and employee, allowing for greater efficiency (matching workforce to immediate work requirements) as well as individual choice (job location, hours, tasks, payment and benefits).

Of course, many traditional jobs and relationships will remain indefinitely. Labour unions and other structures should continue to be an important factor, possibly even gaining in importance as facilitators of workers' transition to new skills and opportunities. Even in older industries, new ICT skills will be required, and the changes elsewhere in the economy will possibly demand new approaches to employee relations.

The most critical implication of these trends is the need for expanded levels of education and training at all levels of society, in all industries. It is estimated that South Africa already faces a shortage of some 9,000 ICT professionals over the next five years [7], a problem that could be exacerbated by a "brain drain" of skilled workers emigrating to other countries where income and opportunities may be greater. Skills in using computers, the Internet, telecommunications and related technologies need to be part of the core curriculum for schools, beginning at the primary level, through universities and graduate programmes. In the interests of overcoming inequities in society, such training should focus especially on the needs of women, people with disabilities, and other disadvantaged groups, through a combination of public programmes and industry-sponsored initiatives.

One of the ways in which the increasing shortage of ICT professionals might be addressed is in fresh and creative approaches to increasing the attractiveness of working in South Africa. The advantages of working in South Africa, as opposed to other countries, need to be identified and marketed actively to this sector of the labour market.

7.4 Government as model user

Government agencies have a unique opportunity to promote e-commerce benefits by "practising what they preach": implementing advanced information technologies to support and manage their official activities. Such government application of ICT in a variety of settings could serve two main purposes, namely –

- to improve the quality and cost-effectiveness of government operations; and
- to establish a foundation for development of ICT applications in the private sector.

Government use of ICTs can benefit the public in many ways. Just as for private businesses, automation of labour-intensive, data-oriented tasks can save time and money, freeing government employees to conduct other, more value-added tasks. Communications technology can give citizens easier access to information and services, and enable them to participate more effectively in the democratic process. With the establishment of common databases and Intranet applications, different government departments can co-ordinate their functions more effectively, thereby saving costs and improving services.

Broader benefits still should be achievable through the government's role in pioneering the extended use of ICTs, in purchasing equipment, software, and services, and in supporting training and education programmes. If the government's procurement practices were to make direct use of e-commerce techniques such as on-line ordering and funds transfers, this would also help to establish these activities as both legitimate and reliable.

There are numerous models for public–private partnership in promoting development of new technologies and even industries, without imposing excessive bureaucratic restrictions on private companies or inhibiting market competition and innovation. Joint participation in studies, research, cross-sectoral programmes, and even investment ventures should be encouraged. The public would stand to benefit from co-operation between industry and government as new technologies are applied to corporate and official operations and relationships.

7.5 Current policy and initiatives in South Africa

The new government of South Africa has made it one of its central aims to eliminate social and economic inequities and to create new opportunities for the country's most disadvantaged population sectors (see Section I). The Reconstruction and Development Programme (RDP) established by the Mandela administration defined the following among its fundamental goals [8]:

- to provide universal, affordable access for all as soon as possible within a sustainable and viable telecommunications system;
- to develop a modern and integrated telecommunications and ITC system that is capable of enhancing, improving affordability of and facilitating education, health care, business information, public administration and rural development; and
- to develop a southern African co-operative programme for telecommunications.

President Mbeki has pledged to maintain and reinvigorate the principles of the RDP.

These objectives have been the foundation of the strategic policies of the Department of Communications as well as other public sector institutions. As mentioned in the previous section, the DoC has launched an aggressive series of initiatives under the collective label of the "Info.Com 2025" programme, which seeks to achieve broad-based growth and equitable

development through communications and information technologies. Some of the key elements of the Info.Com programme include –

- a Commission for Information Communications Technology (CICT);
- the Universal Service Agency (USA) telecentre projects;
- Public Information Terminals (PITs), Internet-2000, and Web Internet Lab: projects designed for rapid expansion of access to the Internet and for experimentation with Internet applications;
- TradeNet: liaison with the Department of Trade and Industry to promote international trade opportunities via e-commerce; and
- Houwteq: a national training institute for study, research, and development in technology and software.

Many firms in the private sector have embraced the goals of the RDP and the opportunities of e-commerce to expand their own business, while maximising benefits to society as a whole. For example, the South African Integrated Development Initiative (SAIDI) was recently formed as a consortium of hi-tech and development-oriented companies. Its purpose is to work with local communities and the government to support sustainable, integrated development projects. The intended SAIDI focus is to provide community projects with access to technology, training, funding and business expertise across all the provinces.

Other related initiatives include –

- the South African IT Strategy (SAITIS) Project, a three-year joint project between the Department of Trade and Industry and the Canadian International Development Agency (CIDA) with the objective of developing a strong South African IT industry;
- the Department of Labour Electronic One Stop Service Infrastructure, aimed at achieving single-window delivery of services to its constituents;
- the development of the science and technology white paper by the Department of Arts, Culture, Science and Technology, with an emphasis on harnessing the information revolution;
- the development of the telecommunications white paper by the Department of Communication; and
- the initiative by the Department of Welfare to re-engineer its welfare payment system.

These and other initiatives reflect the way in which government is responding to the challenge of using enabling technologies and new business paradigms to improve its service delivery and to create enabling environments. These initiatives need to be co-ordinated through relevant policy development by a cross-section of stakeholders.

7.6 Policy response options and questions

As indicated above, there are numerous ways in which the government can contribute directly and indirectly to maximising the benefits (and minimising the risks) of e-commerce, and of information and communications technologies. The South African government and the private sector have taken steps in these directions already, and should continue to explore every avenue to take advantage of technological change as an engine for social equity and economic growth.

One initiative that could be considered for inter-departmental and public-private co-operation is to study and promote the benefits of e-commerce in South Africa. An agency could be established for e-commerce, with a mandate (similar to the Universal Service Agency's mandate for

telecommunications) to promote widespread access to and use of e-commerce technologies, especially among disadvantaged groups.

Such an agency could have a five-year initial term, with funding provided jointly by government and private industry. It would concentrate on bringing together elements of private industry, universities, research centres and government departments (similar to the SAIDI described above) to identify opportunities, pool resources, and promote specific development projects. This entity could also serve as a public "think tank" to monitor industrial and technological trends worldwide and thus provide market intelligence and data to all companies involved in South African e-commerce.

South African industry and government has to consider these and other options and to devise practical programmes to help small businesses and entrepreneurs as well as large national companies to realise the potential benefits offered by e-commerce technologies. This effort should be accompanied by public discussion of the following policy questions, among others:

- What are the main business opportunities and advantages in South Africa that can be exploited through the digital medium, for export and trade development purposes?
- Which government programmes and departments should take the lead (together with universities and industry) in promoting broad-based education and training initiatives, and what funding mechanisms can be employed to support these?
- What specific government services can be offered electronically in the short term, both to support of the overall e-commerce market and to improve the effectiveness and efficiency of those services?
- How significant are the short- and medium-term impacts of new e-commerce industry developments likely to be on the present workforce, in terms of both job losses and job creation?
- What types of resources should be devoted to retraining and compensation for workers at risk due to automation, shifting of jobs offshore, or elimination of the need for certain intermediary activities in an e-commerce environment?
- In what proportions should government and private companies share the responsibility and cost for easing the transformation of the workforce through these types of assistance programmes?

8. Conclusion: The Way Forward

It is clear that the issues and initiatives that will need to be debated and addressed by South Africa to create an enabling framework for Electronic Commerce, have far reaching implications and impact. Thus a significant effort will be required, that must include a host of stakeholders, to ensure that policies and processes are put in place that address the needs, whilst effecting this in the shortest possible time.

The policy process will be launched officially by the Minister of Communications to begin a process of discussion and allow for public participation and debates. All interested stakeholders, including all sectors of industry, community structures, academic institutions, government departments and agencies, non-governmental organisations, grassroots organisations, multilateral organisations, trade missions, organised labour, various interest groups and associations, individuals and society at large, are invited to participate in the discussion. Written responses, comments and views on the issues raised in this document should be forwarded to Ms Dillo Lehlokoe at the following address:

Department of Communications
Private Bag X860
399 Duncan Street
Hatfield
Pretoria
0001

Tel: +27 12 427 8037
Fax: +27 12 427 8085
e-mail: dillo@doc.pwv.gov.za

The address of the website for the E-Commerce Debate and Discussion in South Africa is: http:/ecom-debate.co.za.

---

1 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, http://www.wassenaar.org.

2 *European Union Directive 95/46/EC*, Official Journal of the European Communities, 23 November 1995, No L. 281, p. 31.

3 *European Union Directive 95/46/EC*, unofficial version: http://www.cdt.org/ privacy/eudirective/EU_Directive_.html.

4 *Electronic Commerce Due Diligence Report*, Edward Nathan & Friedland Inc, Johannesburg, South Africa, May 1999.

5 Report prepared for Department of Communication, Telecommunications Sector Consultancy for Specialised Policy Advice: David N. Townsend & Associates, December 1997.

6 Electronic Money Position Paper NPS 11/99, South African Reserve Bank, National Payment System Division, April 1999.

7 HSRC Report: *Investigation into the Demand for and Supply of high level Human Resources for the Telecommunications Industry*, September 1998.

8 Reconstruction and Development Programme, 1994.