4 Policy Options: The Digital Society

4.1 Introduction

The World Summit of Information Societies (WSIS) Plan of Action emphasises the key role electronic communications networks can play in enabling the implementation of development strategies and highlights that in order to harness this, governments should develop and implement "*forward looking and sustainable national e-strategies*" in dialogue with the private sector and civil society. The Policy Options and issues put forward in this Chapter are in many ways focused on further developing the principles and strategies necessary to finalise such a holistic national e-strategy to ensure a coordinated approach to building an information society. It builds on existing strategies, including South Africa's national broadband policy, '*South Africa Connect: Creating opportunities, Ensuring Inclusion*", adopted in 2013

It is recognised that ICTs are a tool in developing a dynamic information society and that this is dependent to a large extent on universal service and access to the Internet and to other ICTs. It is also crucial that government policies ensure all South Africans have the skills and opportunities to meaningfully engage with services and products available online, via mobile devices or on platforms such as the Digital Terrestrial Television (DTT) platform. South Africans must also have opportunities and the skills to create content and offer services and products themselves and know how to protect themselves online.

Promotion of universal access to affordable broadband and other platforms is, however, dealt with in Chapter Three (Policy Options: Infrastructure and Services), skills development in Chapter Six (Policy Options - Industry Growth) and audio-visual content (including broadcasting and broadcasting-like content) in Chapter Five. The SA Post Office (SAPO) can assist in extending digital services. While these are referred to where necessary (e.g. regarding accreditation of electronic signatures), Policy Options for Infrastructure and Services (Chapter Three) deals extensively with the role of SAPO in general including its role in promoting and supporting e-government, e-commerce and other services.

This Chapter/Policy Options Paper focuses therefore on digital services (including e-government services), the digital economy (and e-commerce) and the issues necessary to promote trust and confidence (including privacy provisions, protection of consumers, cybercrime and cybersecurity). The primary focus is on the ambit of the DTPS and its roles and responsibilities as well as those of the agencies aligned to it. Given that a dynamic information and knowledge society relies on cooperation and coordination between all spheres of government, the private sector, civil society and citizens, issues related to other entities are also dealt with to some extent with a focus on how to facilitate the partnerships necessary to achieving the vision.

The terms e-services, e-commerce and e-society are used to cover the use of a range of digital technologies and platforms including the Internet, mobile phones and other platforms, for example, DTT. It also in this context refers to use of SMS and other such services.

4.2 Context

4.2.1 National policies

4.2.1.1 National Cyber Security Framework

Cabinet approved the National Cyber Security Framework in March 2012 and the DTPS established the National Cybersecurity Advisory Council in 2013 in terms of this to advise government on cybersecurity policies. The aim of the Framework is to:

- Promote a cybersecurity culture and facilitate compliance with minimum security standards;
- Strengthen mechanisms in place to prevent and address cybercrime, cyber warfare, cyber terrorism, and other related issues;
- Establish public-private and societal partnerships within South Africa and internationally to strengthen awareness and enforcement;
- Ensure the protection of national critical information infrastructure;
- Promote and ensure a comprehensive legal framework governing cyberspace; and
- Ensure adequate national capacity to develop and protect South Africa's cyberspace

A number of government departments are involved in the implementation of the Framework under the oversight of the Cabinet Justice, Crime Prevention and Security Cluster. The DTPS is specifically tasked with establishing a National Cybersecurity Advisory Council, Cybersecurity Hub as well as the national Computer Security Incident Response Team (CSIRT).

4.2.1.2 Electronic Government: The Digital Future: A Public Service IT Policy Framework

This policy on e-government was developed by the Department of Public Service and Administration (DPSA) in 2001. It is currently being reviewed.

4.2.1.3 King III and Companies Act

The 2009 King Report on Governance for South Africa and the King Code of Governance Principles (collectively referred to as King III) has a full chapter on information technology governance recognising that IT is fundamental to the growth of many organisations but also poses significant risks. It states therefore that IT should be governed at a Board level. It requires that a specific independent audit on IT is conducted.

4.2.1.4 Other policies

A number of other policies are relevant to building a digital society, including the Minimum Information Security Standards and the Minimum Operability Standards. Both need to be updated but are in place.

4.2.2 Relevant laws

Provisions related to the digital economy and knowledge society are spread across many different laws, including:

- E-communications are currently regulated by the Electronic Communications and Transactions Act, 2002 ("ECTA" or "ECT Act") which provides for "*the facilitation and regulation of electronic communications and transactions*". Amendments to the Independent Communications Authority of South Africa Act introduced in 2014 give the regulator some responsibilities in relation to electronic transactions including monitoring the implementation of ECTA. Amendments to the ECT Act were drafted in 2012 but have yet to be promulgated, pending the outcomes of the ICT Policy Review

process. A number of regulations have been promulgated under the Act, including the Alternative Dispute Resolution Regulations.[1]

- The Promotion of Access to Information Act, no 2 of 2000 ("PAIA") which gives effect to the constitutional right to access to information.
- The Public Service Act, 1994 (amended in 2007) states that the Minister of Public Service and Administration is responsible for information management in Government and for electronic government ("*the use of information and communication technologies in the public service to improve its internal functioning and to render services to the public*").
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act, no 70 of 2002.
- The Film and Publications Act, no 65 of 1996 which sets out the regulatory framework for film and publications by means of "*classification, the imposition of age restrictions, and giving of consumer advice*" and bans the exploitative use of children in pornographic publications, films or on the internet. The Film and Publications Board (FPB) established in terms of the Act has indicated that an amendment process is underway "*to allow for better regulation of online content distribution*".[2]
- The Consumer Protection Act, no 68 of 2008 which sets out an overarching framework for consumer protection in South Africa.
- The Protection of Personal Information Act, no 4 of 2013 regulates how personal information can be processed.
- The Income Tax Act, no 58 of 1962 deals with the levying of income tax on all individuals either residing or earning their income in South Africa along with the Tax Administration Act, 28 of 2011 and the 2014 "*Rules for Electronic Communications prescribed under the Act*".
- A range of laws related to copyright and intellectual property protection such as the Copyright Act (no 98 of 1978), the Patents Act (no 57 of 1978), the Trade Marks Act (no 194 of 1993), the Intellectual Property from Publicly Financed Research and Development Act (no 51 of 2008) and the Intellectual Property Rights Amendment Act (no 38 of 1997). The Intellectual Property Laws Amendment Act, 28 of 2013 (IPLAA) was assented to by the President in December 2013 but is not yet in effect. It focuses on the protection of indigenous knowledge.
- The Protection from Harassment Act, no 17 of 2011, provides easy, quick and inexpensive mechanisms for victims of harassment to get a court order to protect themselves. The Act includes unwanted verbal or written communication via electronic communications in its definition of harassment.
- The National Gambling Act, No 7 of 2004
- The Protection of Administrative Justice Act, no 3 of 2000, sets out provisions to ensure the constitutional right to administrative justice.

4.2.3 International Treaties and Agreements

A number of International, regional and SADC treaties, protocols, agreements and policies are of relevance, including:

- The ITU/UN **World Summit on the Information Society** to "*harness the potential of knowledge and technology for promoting the goals of the United Nations Millennium Declaration and to find effective and innovative ways to put this potential at the service of development for all*". It was held in two phases, and included governments, members of civil society and of the private sector:

[1] Department of Communications, "Electronic Communications and Transactions Act 2002: Alternative Dispute Resolution Regulations", 22 November 2006, http://www.domaindisputes.co.za/downloads/AlternativeDisputeResolutionRegulations.pdf

[2] Ellipsis, "The Film & Publications Board and online content regulation", 13 September 2014, http://www.ellipsis.co.za/the-film-publications-board-and-online-content-regulation/

    - The Geneva Phase (2003) adopted the Geneva Declaration of Principles and the Geneva Plan of Action which outline a clear statement of political will and concrete steps to establish the foundations for an Information Society for all.
    - The Tunis Phase (2005) adopted the Tunis Commitment and Tunis Agenda for the Information Society which considered Internet governance, financing mechanisms and follow up implementation of the commitments made in the two summits. [3]
- The **Budapest Convention on Cybercrime, 2001,** is an international treaty dealing with crimes committed via the Internet and other computer networks, including infringements of copyright, computer-related fraud, child pornography, hate crimes and violations of network security.
- There are a range of treaties that deal with **intellectual property** issues including the Berne Convention (1978), the Trade Related Aspects of Intellectual Property Rights (TRIPS) of the General Agreement of Trade in Services (GATT), the World Intellectual Property Organisation Treaty (WIPO Treaty), and a number of other treaties administered by WIPO such the WIPO Performance and Phonograms Treaty
- The **African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa** which was brought into law in 2014 indicates that it is aimed at harmonising laws in African countries dealing with e-commerce, personal data protection, cyber-security promotion and cyber-crime control.[4]
- The **Southern African Development Community** ICT Ministers adopted **an e-SADC Strategy** in May 2010. As part of the implementation of the strategy, a **SADC e-Commerce Strategy and Action Plan** aimed at enhancing regional trade through e-Commerce was developed and adopted in November 2012. Among other things, the Strategy raises the need to develop a holistic framework to raise awareness on cybersecurity and cybercrime issues, establish national and regional Computer Incident Response Teams (CIRTs), and collect and share cybercrime statistics/indicators for a SADC Annual Cybercrime Reports.
- SADC has also developed **Harmonised Cyber Security Model Laws**, including **e-Transactions/e-Commerce, Data Protection and Cybercrime model laws**.
- The **United Nations Commission on International Trade Law** (UNCITRAL) specialises in commercial law reform and the harmonisation of rules on international business. It has formulated a range of related conventions, model laws and rules.

4.3 Overall policy approach

ICTs are an important tool for sustainable development and economic growth. Government, however, will need to provide strong leadership if the benefits of new technologies to social, cultural and economic development are to be realised.

Probably the most important principle that underpins all policy approaches in this Chapter is that of ensuring inclusion and that all South Africans can access and interact with the benefits of building a digital economy and information society. This is in line with the SA Connect Broadband Policy and the NDP. Inclusive development requires not only access to infrastructure, devices and affordable services, but also that content, information, products, services and applications developed are relevant to the most disadvantaged sectors of society, support welfare and entrepreneurship and are available in a range of South African languages. E-government and other e-services and applications will further have to consider the different technologies used by different sectors of

[3] http://www.itu.int/wsis/basic/about.html
[4] http://au.int/en/cyberlegislation

society and, for example, design applications recognising that many users will be, at least in the medium term, reliant on mobile technology and less sophisticated mobile phones. The costs of accessing data will also have to be taken into account.

Accessibility by persons with disabilities is another critical aspect of inclusion to address in ensuring universal access and should be built into all policy approaches and be considered in developing innovative services and solutions.

As emphasised in the National Broadband Policy, open access and the promotion of interoperable platforms and standards should be another primary focus of government policy if the full benefits of the digital society are to be reaped, and fair competition between new and existing companies and large firms and SMMEs facilitated. The impact of new technologies and the Internet on competition will need to be continually assessed to address any new challenges that might arise.

Given the above, policy will need to be flexible, people-centred, rights-based and balance the need to promote innovation with that of protecting users. Creative policy interventions will have to be developed in order to protect individual rights while ensuring regulation does not inadvertently constrain economic development. Finally as noted in several submissions to the Green Paper, digital technologies and e-strategies are not ends, but tools to assist the public, private and non-governmental sectors to fulfil their transformation goals.[5]

4.3.1 Government approach

There are currently a number of different e-policies and strategies in place. The DPSA is responsible for e-government strategies and developed a national e-government policy in 2001 (The Digital Future). The ECT Act meanwhile states that the Minister of Telecommunications and Postal Services should lead the development of a three year national e-strategy and monitor its implementation. It states that this should include provisions on e-government strategies developed in consultation with the Minister of Public Service and Administration, and a national policy for electronic transactions. Such a policy has not been finally adopted by Cabinet, though an Information Society Development (ISAD) plan was developed and approved by Parliament in 2007. In addition, a cybersecurity framework has been developed. and as indicated in the relevant sections below, a draft cybercrime policy is under discussion. Subsequent to this, the NDP has called for the finalisation of a national e-strategy that cuts across government departments and sectors of society.

It is clear that the issues related to building a digital society cut across many different government departments, entities and spheres of government and that there is a need therefore for a holistic overarching approach that would define the different issues and areas to be covered and assign responsibilities for e-government, the development of infrastructure and networks to support strategies, the promotion of a digital society, e-commerce and e-services across society as well as issues on crime and security. Initiatives related to skills development and building of awareness and digital literacy also need to be coordinated to increase their impact.

[5] Submissions that focused on this include those from Cell C, the National Cybersecurity Advisory Council, Sizwe Snail Attorneys, the Western Cape Government ICT Policy and Strategy Directorate, SALGA and several municipalities and the Western Cape Government ICT Policy and Strategy Directorate.

Several submissions highlighted that coordination across a range of government departments and entities is crucial and the need for alignment of the different laws in place. Proposals and options relating to this are dealt with at the end of this Chapter. Research ICT Africa said that an "*integrated national e-strategy*" must "*cut across sectors, government departments, meet the diverse needs of the public sector, the formal sector and the informal sector, foreign investors, start-ups, and citizens where ever they may be*".[6]

Others highlighted that government has a critical role to play not only in developing policies in relation to e-government, e-commerce and e-services, but also in providing South African best practice models in relation to the provision of such services. The SACF, for example, stated that government should lead the way in adopting digital technologies and shifting activities online, showcase achievements of business innovators and develop e-commerce certification certificates. It also proposed that government could through its procurement policies facilitate increased compliance with laws by service providers by, for example, taking into account the ability of the provider and/or technology to protect the privacy and security of customer information.[7]

4.4 E-Government

E-government is "*the use of ICT and its application by the government for the provision of information and public services to the people*".[8] It includes the use of technologies to make government work processes more efficient, strengthen public service delivery and enhance communication channels with citizens:

- Government to Government programmes (G2G);
- Government to Citizen programmes (G2C);
- Citizen to Government programmes (C2G); and
- Government to Business programmes (G2B).

The UN in its latest e-government survey states that there are four stages to e-government:

- Stage One – Emerging Presence: E-government presents information which is limited and basic. It includes an official web-site and links to individual web-sites.
- Stage Two – Enhanced Presence: Online services of government include interactive services such as downloadable forms.
- Stage Three – Transactional Presence: E-government allows for two-way interaction including e-tax filing for example and systems to allow for citizens to submit applications online 24/7.
- Stage Four – Networked Presence includes an integration of all programmes enabling participatory decision-making and involvement of society in a two-way open dialogue.

South Africa ranked 93 out of the 193 countries included in the UN survey (up from 101 in the 2012 survey) and 97 in the e-Participation Index.[9]

As highlighted previously, the Minister of Public Service and Administration is responsible for government's overall e-government strategy in terms of the Public Service Act. The DPSA developed

[6] Research ICT Africa, Green Paper submission, page 7
[7] SACF, Green Paper submission, page 28
[8] United Nations, "E-government Survey 2014", Executive Summary, page 2, http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/0ExecutiveSummary.pdf
[9] UN Public Administration Country Studies, "UN E-Government survey 2014", http://unpan3.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014

an e-government strategy in 2001 and is currently reviewing this. The ECT Act notes that an e-strategy must incorporate an e-government strategy and plan and emphasises the need for consultation and coordination between the DPSA and DTPS and other government departments, spheres and public entities. An Intergovernmental Task Team has been established to develop the "National e-Government Strategy 2030" in recognition of this. It is led by the DPSA and the DTPS is part of the team.

A number of structures, policies, programmes and activities have been put in place or are in the process of being developed in order to assist in delivering and enhancing e-government services:

- The SA Connect Broadband Policy emphasises the need to pool public sector demand for broadband and to procure "*high-capacity and future-proof network capacity at more affordable rates to address public sector broadband requirements*".[10] The National Broadband Advisory Council was established in March 2014 to advise the Minister on implementation of the policy.
- The Presidential Infrastructure Coordinating Commission's (PICC) SIPs 15 focuses on expanding access to communication technology and extending broadband coverage to all households by 2020 by establishing core Points of Presence in district municipalities, extending Broadband Infraco's fibre networks across provinces and ensuring penetration into rural areas.[11]
- In order to facilitate the above two policies and programmes of action, state owned entities are undergoing a rationalisation process. SITA and Broadband Infraco have been transferred to the DTPS.
- The Government IT Officers Council (GITOC) was formed in 2000 as an advisory body to government and facilitates effective and efficient information technology and information management in the public service.

There are numerous applications running in different government departments and entities, from one-stop web portals to electronic transactional services such as those set up by the South African Revenue Services for tax. Some municipalities have also introduced mobile applications to allow for reporting of service delivery problems. Other e-government initiatives include e-Natis online vehicle and transport management system, the e-justice programme to improve judicial procedures, the e-Hanis programme to streamline and integrate personal identification data across government departments and the National Automated Archival Information Retrieval System to facilitate access to public archived records.

In further developing e-government services, it is important that government develop specific interventions, including social media, to promote participation by citizens in governance and monitoring of service delivery. There is a need to develop standardised approaches to such engagement, and ensure that government not only develops tools to promote citizen engagement but also mechanisms to ensure that contributions from the public are engaged with and, for example, problems identified by organisations and individuals addressed.

A number of stakeholders made proposals in response to the Green Paper emphasising the necessity of strengthening coordination of e-government services and ensuring harmonisation of policies. Submissions highlighted the need for government to use ICTs as a catalyst to improve the quality

[10] Department of Communications, "South Africa Connect: Digital Opportunities, Ensuring Inclusion: South Africa's Broadband Policy", page 30

[11] PICC, "A summary of the South African National Infrastructure Plan", page 23, http://www.gov.za/sites/www.gov.za/files/PICC_Final.pdf

and cost-effectiveness of government operations and to drive improvement in service delivery. Stakeholders proposed that the DPSA and DTPS work more closely on these issues, that a range of enforceable norms and standards on e-government and information management be developed and that SITA's role is reviewed. It was suggested that SITA focus on design development and implementation support for government entities with limited ICT capabilities and develops wholesale business models to improve procurement efficiency across government.[12]

The South African Local Government Agency (SALGA) and a number of individual municipalities also made submissions focusing on the need to support implementation of e-government services at a local level. SALGA emphasised the need for any e-government strategies, policies and implementation plans to specifically consider the needs of local government and its role in delivering services at a local level. It said that all related policies need to be reviewed given changes in technology brought about by convergence and proposed that specific policies on open data (digital information available at no cost through free internet connectivity to key sites) must be incorporated. [13]

In a supplementary submission, SALGA noted that there are very different capacities in local municipalities to integrate ICT into their plans and ensure that technology addresses efficiency within local government and is used to improve services to the public. While many metros have implemented ICT strategies to support development initiatives, district and local municipalities often have no ICT strategy and struggle to build efficient and effective financial and administration systems.

The Municipality of Matlosana in its response stated that any review of e-government initiatives should also include the Municipal Structures Act of 1998, the Municipal Systems Act of 2000 and local government performance management regulations to incorporate provisions on how ICT in local government should be governed, regulated, monitored and evaluated. It also proposed that:

- Training for ICT personnel in municipalities be standardised;
- Training service providers should be regulated to ensure accreditation in line with NQF requirements.
- Executive training in the importance of ICTs be introduced.
- Mechanisms be put in place to attract ICT expertise at a local government level.[14]

Snail Attorneys meanwhile noted that it was important in developing a trusted and secure e-commerce environment to urgently use digital technologies to address challenges in the justice system. An e-justice system focusing on improving the efficiency of the justice system would address some of the delays currently beleaguering prosecution such as the loss of court files and dockets.[15]

POLICY OPTIONS: E-GOVERNMENT STRATEGY

- There is clearly a need to update the existing e-government strategies as well as align and update related regulations and standards. This will assist in determining public sector need, and pooling this

[12] Submissions on this were made by a number of entities including National Treasury, the Progressive Professionals Forum (PPF), Snail Attorneys and the NCAC
[13] SALGA, Green Paper submission, pages 4-5
[14] City of Motlasana, Green Paper submission, pages 7-10
[15] Snail Attorneys, Green Paper submission, page 2

as indicated in the National Broadband Policy. Currently both the DPSA and DTPS have a role to play in this.

- There is also clearly a need to develop additional norms and standards, both on technology solutions and content approaches to promote openness (including open data policies).
- Linked to this are questions about what issues and areas an e-Government strategy should address. It is proposed that key areas include e-administration (ICTs to improve the internal functioning of government institutions), e-service delivery (public investment to deliver public services and information to the public), and e-participation (tools and mechanisms to enhance interaction and dialogue with the public). A strategy can define these areas and commitments. While some implementation is possible at a national level, provinces, municipalities, individual departments and public entities need to develop their own digital strategies linked to their specific development plans and programmes. These would ultimately need to be integrated into a holistic government portal/s. An overarching e-government strategy and implementation plan could indicate key components and approaches to be considered by individual departments, spheres and entities in developing digital plans to support their strategies.
- A policy must also develop tools and mechanisms to ensure that all government services are integrated so that citizens only have to provide information once to receive/access all government services from any public service point. It will have to promote the development of an integration backbone to enable information sharing between government departments, agencies, provinces and municipalities.

Option One: Status quo strengthened

The DTPS is responsible for developing a national overarching e-strategy and implementation plan to be approved by Cabinet and Parliament, including approaches to e-government. The DPSA and the DTPS would work together with other relevant Departments to update the existing e-government strategy. Existing norms and standards (such as MISS and MIOS) would be updated jointly and new norms and standards developed if necessary as part of this, and the e-strategy would determine responsibility for each of these. The e-government strategy should be developed through a consultative process, and include inputs from a range of entities, including representation from provincial and local government, as well as entities such as the National Broadband Advisory Council and SIPs 15. Roles of different entities should be specified in the strategy and associated implementation plan. A White Paper would need to set deadlines for finalisation of this and put in place mechanisms for review and accountability if deadlines are not met.

- **What areas should an e-government strategy focus on?**
- **What norms and standards need to be updated and what additional standards developed?**

Option 2: Using digital technologies to address challenges relating to justice and prosecution of crimes

As suggested above, it is proposed that a specific focus on addressing administrative challenges in the justice and courts system through development of digital technological solutions would be identified as a priority.

- **Do you agree that e-justice systems be identified as a specific priority in relation to e-government services?**

POLICY ISSUES: ROLE OF STATE OWNED COMPANIES

The Government Chief Information Officer situated within the DPSA is responsible for developing IT related policies, regulations, norms and standards. The Government Information Technology Officers Council (GITOC) includes national and provincial IT officers and is responsible for coordinating IT initiatives in government, including e-government, to facilitate service delivery.

The State Information Technology Agency (SITA) was established in 1998 to improve the effectiveness and efficiency of the public sector and facilitate service delivery through the provision of information technology, information systems and related services. In 2014 the Agency was moved from the DPSA to the DTPS. Section 7(6) of the SITA Act also requires the Agency to set standards for the interoperability of information systems and for a comprehensive information systems security environment for departments. SITA is further required in the Act to certify every acquisition of any information technology goods or services by a government department for compliance with the above mentioned standards.

It has been suggested that the role and mandate of SITA be reviewed and that it specifically focus on, for example, design-development and implementation support to all government entities, including to national, provincial and local government with a specific focus on those with limited capacity. It has also been suggested that the mandate of GITOC needs to be strengthened to ensure that it has the powers to oversee implementation of e-government and ICT strategies.

- **How could government ensure better implementation of its e-government objectives?**
- **What role should SITA play?**
- **How could GITOC be strengthened?**

4.4.1 Government e-segments/services

The SIPs 15 programme and the National Broadband Policy have prioritised e-health (including support for the National Health Insurance plan) and e-education as the initial focal points for infrastructure development. This does not negate the need for the development of strategies by other departments and spheres of government but rather highlights the specific initial priorities for infrastructure development. The Minister of Health has finalised an e-health strategy and the education departments have developed a White Policy on e-education.

The **e-health strategy** focuses predominantly on the role ICTs can play in facilitating effective monitoring of the health systems, and roll-out of the National Health Insurance. It highlights that the roll-out of health information systems has been characterised by "*fragmentation and lack of coordination*" and a lack of interoperability between the different systems and outlines how this will be addressed.

The White Paper on **e-Education** (2004) stresses the need for all learners to be equipped with the skills and knowledge to use ICTs confidently:

> *"Every South African learner in the general and further education and training bands will be able to use ICTs confidently and creatively to help develop the skills and knowledge they need to achieve personal goals and to be full participants in the global community by 2013."*

The National Broadband Policy specifies that roll-out of broadband to schools and other educational institutions is a priority in light of this and highlights that the Education Departments have identified the need to use digital technologies to:

- Extend access to educational opportunities across gender, spatial and socio-economic divides and ensure access by persons with disabilities.
- Enable flexible open learning environments including interactive and personalised learning opportunities.
- Extend learning beyond the formal schooling system; and
- Streamline administration for teachers and administrators and enable assessment and data collection.

The NDP recognises that there are many ways to facilitate this, and highlights the need to "*explore the use of mobile devices such as phones and tablets in distributing learning content".*

The initial emphasis of the DTPS is on facilitating roll-out to all schools and it is working with the SIPs 15 team and the National Broadband Advisory Council on this so that the NDP vision can be realised and *"(high speed broadband will be readily available and incorporated into the design of schools. This will enable greater use of technology in education and enhance the classroom experience for both teachers and students."*

Option One: Status quo

E-health and e-education remain the priorities.

Option Two: Extended priorities

The policies extend priorities to all frontline citizen interacting Departments.

- **Do you think the priorities should be extended?**
- **What targets could be set in policy in relation to this?**

4.4.2 Promoting access to information and open government data

Digital technologies can play a key role in promoting access to information, both by improving records management and by providing open access to key public information (open data policies). Open government data policies would emphasise that information and data are made available for "*everyone to access, reuse and redistribute without any restrictions*".[16] Open government data therefore is a means not only to facilitate the right of access to information, but to enable others (including the private sector, communities, academics, research institutions and civil society organisations) to conduct further analysis on such data. This is seen as promoting accountability, transparency and allowing for informed participation in the development of public policies.

The possibilities and benefits of open data are growing given the increasing pools of data available known as Big Data. Big Data makes it possible to integrate and analyse data sets from various data sources, thereby providing an opportunity to extract potentially valuable information in an automated and cost-efficient way. This provides an opportunity for the public sector, as an

[16] United Nations Department of Economic and Social Affairs, "Guidelines on Open Government Data for Citizen Engagement", 2013, http://workspace.unpan.org/sites/Internet/Documents/Guidenlines%20on%20OGDCE%20May17%202013.pdf

important source and user of data, to exploit the full potential of the data it generates and collects, as well as the potential of data generated elsewhere. Big data could also assist in improving internal security and law enforcement. For example, government can exploit non-traditional data sources such as SMS and social media to complement official crime statistics. Big Data can also benefit other industries including the private sector, health care, utilities and logistics and transport.

In his submission on the Green Paper, Jean-Paul Van Belle, from the University of Cape Town's Department of Information Systems, stated that he thought it critical that a new policy specifically include commitments to open government data. He said that this would not only promote transparency but assist the "*public and research community… in researching, creatively addressing and possibly relieving social ills*".

While there is not a national open data policy, the principle of transparency is captured in many government standards and practices, and, for example, organisations such as Statistics South Africa have data available for use and reuse by any member of the public and have introduced tools to assist in extracting and analysing such data. The Independent Electoral Commission provides detailed information on its website on voting patterns at a national, provincial and municipal level, and the City of Cape Town has recently published an open data policy.

- **Is there a need for a specific national open data policy?**
- **If so, what do you propose should be included in such a policy?**
- **How can government ensure that policies relating to open data are implemented across all government and public entities and spheres?**

4.4.3 Protecting information

It is also crucial that the state puts in place adequate measure to ensure the integrity of digital public information to protect it from being manipulated or changed, to ensure confidentiality of, for example, personal records and to ensure there are mechanisms in place to ensure the security of sensitive information within the framework of the Public Access to Information Act. Currently, there are no common standards or mechanisms in place across government to address the protection of digital information. While some departments and different government entities have developed their own solutions to this, these are not necessarily interoperable across all government entities.

A number of norms have been put in place:

- The Minimum Information Security Standards (MISS) were developed in 1992 but are outdated. These address information security within Government. Draft National Information Security Regulations were prepared seven years ago but have never been published.
- The Minimum Interoperability Standards (MIOS) have been updated more regularly by SITA (most recently in 2009) but several submissions on the Green Paper stated that these are routinely ignored. While various solutions exist for the encryption of data, they are generally regarded as too cumbersome to set up, manage and use on an ongoing basis. There is therefore a need to ensure interoperability, promote electronic and secure digital records management and ensure adherence to policies.

There is clearly a need for the finalisation of a government-wide IT governance framework and to update all standards and rules. The need for this has been emphasised by the Auditor General which

conducts audits on management of IT vulnerabilities and risks across government and public entities. Public entities and state owned companies are also subject to the Companies Act and the King III Code which highlight the importance of IT governance and risk management. The DPSA "Protocol on Corporate Governance in the Public Sector" further reinforces this.

POLICY OPTIONS

It is essential that all policies, norms and standards to protect digital information and data are reviewed and mechanisms put in place to ensure they are applied and implemented.

- **How could the overarching ICT government framework be improved?**
- **How can policy protect the integrity and security of government digital information while promoting open data policies?**
- **How can this be coordinated across Government to ensure the involvement of key institutions and stakeholders, including the DTPS, DPSA, SITA, GITOC etc.?**

4.4.4 Promotion of access to government e-services and information by persons with disabilities

While other chapters/policy options papers in this Discussion Document deal specifically with access by persons with disabilities to services and content (including, for example, development and promotion of assistive technologies, sign language and audio-description on broadcasting services and training and skills development), this sub-section focuses on the role that government should play in ensuring access and inclusion. ICTs can be used to promote inclusion within the public service as well as ensure access to government services and information by people with disabilities.

In line with this the following policy principles are proposed for incorporation into a final policy, and in related policies and implementation plans:

- Software and operating systems developed to improve administrative efficiency within government must incorporate mechanisms to ensure access and easy use by persons with disabilities working within the public sector.
- In its procurement of hardware and software, government should require service providers to ensure accessibility and compliance with universal standards. This will assist not only government as it is a major procurer of hardware and software and therefore such requirements will encourage suppliers to ensure access and compliance with universal standards more generally.
- Systems should be introduced across government to ensure integration of data regarding a person's disability to avoid the need to recapture the same data as the person moves from one service point to the next.
- In developing e-government services and solutions, government should both specifically consider how it can use ICTs to promote access by people with disabilities to government services and must ensure all e-government services provided by it are accessible.
- Government must also set guidelines and standards in line with recognised Web Content Accessibility Guidelines to ensure access to all public websites.

In order to facilitate the above, it is crucial that any coordinating structure/s involve organisations of persons with disabilities to ensure their needs are integrated into all e-strategies, e-government policies and other relevant frameworks.

- **Are there other options which should be incorporated into government strategies, policies, standards and frameworks?**
- **How can policy ensure that the needs of persons with disabilities are integrated into planning and implementation of e-government services?**

4.5 The digital economy and e-commerce

The ECT Act sets out the legal framework that governs e-commerce in South Africa. Government plays a key role in facilitating and enabling e-commerce and creating an environment for economic growth. An effective e-commerce framework can, for example, allow for greater access to local and international markets by individuals and the public or private sectors and promote SMME development by facilitating easier and cheaper access by providers to different markets and customers (including local and international buyers). E-commerce can also reduce expenditure in the value chain from supplier to end-user, resulting in lower prices for the consumer and increase efficiency and ease of use of financial transactions with mobile banking. It incorporates:

- Business to-business transactions (B2B);
- Business to customer products and services (B2C);
- Business to government provision (B2G); and
- Consumer-to-consumer transactions (C2C)

There are thus essentially three different possible players involved in e-commerce: The buyer (an individual, public entity, organisation or enterprise), the seller (an individual, organisation, public entity or enterprise) and manufacturer (the individual or entity that produces the product or service). Sellers can offer services directly to customers/users or to a wholesaler/intermediary. The manufacturer can sell to retailers, wholesalers or directly to customers.

The ECT Act it is recognised needs to be updated and amended to address challenges and potential conflicts with other legislation. An Amendment Bill was drafted in 2012 and will be finalised in line with policies developed through this policy review process and to ensure harmonisation with other laws and policies (including, for example, cybercrime and cybersecurity policies, the POPI and Consumer Protection Acts).

An enabling e-commerce environment further recognises that there are a range of different government departments, public entities and private and non-governmental organisations that need to work together in developing a dynamic digital economy. This section deals specifically with the provisions of the ECT Act and with policies that need to be adopted to promote this. As issues relating to promoting trust and security (including provisions to deal with cybercrime, consumer protection and protection of children) relate to both the e-government and e-commerce sectors, these are dealt with in a separate section below.

Research conducted for the ICT Policy Review process as well as submissions by stakeholders to the Green Paper highlighted a number of specific issues as dealt with below.

4.5.1 Legislative duplications and contradictions

There are numerous duplications and contradictions between the ECT Act and other laws and regulations. These include:

- Contradictions between the ECT Act, the regulations to the Companies Act and the Uniform Rules of Court. on methods and timeframes for delivery of documents
- Contradictory definitions and approaches to critical databases/information infrastructure between, for example, the ECT Act, the Regulation of Interception of Communications and Provision of Communication-related Information Act, the SITA Act and the Protection of Constitutional Democracy against Terrorist and related Activities Act of 2004.
- Different provisions on cooling off periods, SPAM and marketing in the Consumer Protection Act and the ECT Act.

Once the White Paper is adopted by Cabinet, it will be necessary to amend the ECT Act to bring this in line with new policies, and for the South African Law Reform Commission to conduct a thorough review to ensure alignment across all legislation.

4.5.2 Electronic Transaction Framework: Electronic signatures

Several submissions were made on ways to improve the general framework and the accreditation process for electronic signature service providers. The ECT Act makes the DTPS responsible for accreditation of electronic signature service providers. Regulations on the accreditation of signatures and the process for accreditation of authentication service providers were published in 2007 by the Minister. Two service providers have been accredited by the DTPS: LAWtrust and SAPO.

The NCAC in its submission said that the system in place is inadequate. It said that the Post Office, for example, had taken more than ten years to accredit service providers and that the "entrenchment" of a government agency as the preferred provider should be reconsidered. The main problem, it highlighted, has been limited market acceptance due to: Limited awareness of the relevance of e-signatures, inconsistencies in the legislation and the application of the legal framework, exacerbated by the mixed role of DTPS as both policy-maker and implementer.[17]

Other submissions the Green Paper also raised concerns about the overall framework, including overlaps in different laws (e.g. privacy, copyright and consumer protection laws) and laws which they said hindered e-commerce development (e.g. laws relating to taxation or trade).[18]

Research conducted indicated that the current limitations in law should be reviewed. Schedule 2 to the Act states that the law will not give validity to transactions relating to immovable property, leases on immovable property of longer than 20 years, wills and codicils and bills of exchange as determined in the Exchange Act (for e.g. cheques). Given that new technologies have resulted in digital signatures being regarded in many instances as superior to manuscript signatures, as they do not allow for any alteration of electronically signed documents, these limitations should be reviewed. Research also indicated that the process for accreditation and the requirement that accredited electronic signatures must meet a set South African National Standard (based on the

[17] NCAC, Green Paper submission, pages 7&8
[18] For example, PPF, Green Paper submission

international standard) is regarded as unnecessarily onerous and could result in limited harmonisation with international developments and therefore affect cross-border transactions.

It is noted that the ECT Amendment Bill includes amendments to deal with some of the gaps in the current law, but that these revisions need to be further reviewed once the policy process has been finalised. Some of the gaps addressed in the current Bill include:

- Definitions for electronic transactions, commercial electronic transactions and non-commercial transactions have been proposed for inclusion.
- The definition for electronic signatures has been strengthened and brought in line with international best practice to ensure that text signed digitally cannot be altered.
- Provisions have also tried to address the specific requirements of different sectors and, for example, the need for high requirements for the banking sector but simplified, though still credible, requirements for SMME's.
- Updates to the law in line with the Consumer Protection Act.

POLICY OPTIONS: ELECTRONIC SIGNATURES AND DIGITAL TRANSACTIONS

As highlighted, once the policy framework is finalised, the Amendment Bill will be revised in line with policies developed and international best practice. Such a review should consider all related laws to ensure there is alignment between different legislation, and remove overlaps and conflicts, if any.

- **Stakeholders are invited to propose specific amendments to the existing law that are not covered in the related Amendment Bill.**

Option One: Status quo regarding accreditation of electronic signatures is strengthened

The existing framework provided for in law would continue – i.e. the DTPS remains the Accreditation Authority, but provisions in the law would be reviewed to ensure harmonisation with international best practice, recognise the needs of different sectors (e.g. banks versus SMMEs) and assess the ongoing relevance of exceptions in the law given advancements in digital signatures.

Option Two: A separate entity is appointed as the Accreditation authority

As with the above, current weaknesses in the law limiting harmonisation with international best practice would be addressed, but the policy and law would provide for the appointment of an Accreditation Authority outside of the DTPS.

- **Please indicate your preferred option. Note that the options are not exclusive and suggested alternatives are welcomed.**
- **Please elaborate on your proposal and indicate, for example, how you think the current provisions on electronic signatures could be amended to ensure harmonisation with international laws and promote cross-border acceptance.**

4.5.3 Banking and mobile and online payment systems

The introduction of online banking and mobile and online payment systems by banks and other businesses (including mobile operators) has supported growth in e-commerce and assisted end-

users across the country (including those that do not have bank accounts or payment cards) to access resources, products and services.

There is a need to encourage innovation in this area, given its benefits to citizens, the private sector and SMME development. At the same time, policy should address consumer protection issues and ensure consumers know their rights and obligations. It is important in this to recognise that a number of parties may be involved in such transactions (including customers, mobile operators, ISPs and social media) and there are therefore many different payment regimes (e.g. payment charged on mobile phone bills versus credit, debit or pre-paid payment cards). This could result in a lack of clarity regarding who is responsible for addressing any problems and what remedies are available.

While consumer protection and other such laws in South Africa do address these issues to some extent, and if necessary could be strengthened, it is important in this Discussion Paper to consider whether or not an ICT White Paper should address these issues, and to what extent. The role of ICASA as a custodian of the ECT Act and as the regulator of electronic communications should also be considered. Areas which policy could address include:

- Guidelines and/or rules on the need for easy-to-use and secure payment mechanisms and understandable and accessible consumer information on the level of security such mechanisms provide (including terms, conditions and costs of transactions). This should include ensuring information is accessible to persons with disabilities.
- Regulations to protect against fraudulent and misleading commercial practices. This could include partnerships with bodies such as the Advertising Standards Authority of South Africa which is recognised as a self-regulatory body in the EC Act.
- Additional provisions specific to the sectors regulated on dispute resolution and redress.

The NCAC in its submission asked whether or not it would be possible to regulate data-sharing between banks and ISPs/mobile operators "*to enable the prevention and combating of electronic financial crimes*".[19]

There are no policy options in relation to this, as the question really is whether or not there is a need to specifically address issues regarding banking in a policy and what, if any, role ICASA can play in strengthening the protection of consumers.

- **How if at all should a final ICT policy address issues related to online and mobile banking and payment systems?**
- **Should the convergence of mobile communications and banking be regulated?**
- **Could ICASA's role in consumer protection in this regard be enhanced? If so, how?**

4.5.4 Taxation issues

It is recognised that e-commerce raises a number of issues related to taxation and that there will be a need to review all taxation policies in line with this. There is a need to examine, for example, double taxation treaties and international, regional and inter-country agreements on taxation.

[19] NCAC, Green Paper submission, page 16

From a consumer point of view, it is also important to ensure awareness of the implications of customs duties and taxes on the total costs of purchasing goods online from providers outside the country. Many small companies and individuals are not aware of the implications of duty fees and taxes (calculated at an added tax value and not the standard 14% VAT). It has been suggested that there should be more upfront and transparent information regarding this so that users can calculate the costs which will be imposed on collection of items so they can properly assess the competitiveness of such purchases.

The Progressive Professional Forum (PPF) suggested that all taxation and trade laws should be reviewed to address e-commerce issues and to allow consumers to benefit from competitive prices abroad.[20]

While this is not an area that the Minister or Department can address as this is the prerogative of the Minister of Finance, it is recognised that taxation issues are one of the ongoing areas for debate in relation to promotion of a digital economy and digital commerce. Stakeholders are therefore invited to highlight issues that the DTPS and Minister can, if relevant, raise with the Minister of Finance in this regard.

4.5.5 Cross-border flows of information

One of the opportunities arising from digital transactions is the borderless and global nature of the Internet. This allows for South Africans to access goods and services outside of the country and to offer goods and services to a wider base.

There are though inevitably also risks associated with this and therefore there is a need to harmonise rules (including taxation provisions) and mechanisms in place to ensure security and instil trust and confidence through developing common standards for verification, accreditation and approaches to consumer protection. SADC's model laws and e-commerce related frameworks are aimed at addressing this in the region. The ECT Act also makes provision for recognition of accreditation for foreign products and services (section 40).
To realise the opportunities of cross-border trade, and ensure that SMME's can benefit from these, South Africa will need to consider what barriers may exist and how these could be overcome. This will need to be considered together with the Ministry of Trade and Industry and the Ministry of Small Business Development. Such issues and policy positions in relation to these will also need to be raised in regional (SADC), African and international forums.

The Swedish National Board of Trade, a public entity established to promote Swedish trade, conducted a study in 2012 into the specific e-commerce related barriers faced by Swedish companies. The report highlights that many e-commerce entities are small businesses and that some of the challenges faced relate to this as they, for example, often ship a large number of small consignments rather than single larger ones and have limited capacity to research all the trade regulations in the countries they trade in. The report states that the following types of cross-border electronic trading are most common:

[20] PPF, Green Paper submission, page 11

- Goods and/or services are bought over the Internet but delivered in a non-electronic form (i.e. physical books).
- Goods are bought over the Internet and delivered electronically (i.e. music or e-books).
- Electronic services are sold (e.g. a South African individual or company provides editing or accounting services to a business or organisation located in a different country).

The study identified eight barriers:

- Lack of information – It is particularly difficult for small companies to find adequate information about the laws, regulations, procedures and methods in place in other countries.
- Customs barriers create administrative challenges for e-traders and in particular for those that are shipping a large number of small consignments.
- Payments and taxes – Country specific payment solutions and differences in tax regulations create costs and administrative problems for e-commerce.
- Intellectual property rights barriers.
- Cross-border data transfer can be affected by legislation that limits the ability of a business to store and transfer data across borders.
- State controls in some countries on the need for local establishment to register domain names and/or specific encryption methods can restrict cross-border trade.
- Other barriers: those identified in the study include roaming charges, certification of products, lack of standards, rules of origin etc. [21]

The PPF in its Green Paper submission highlighted the challenges of cross-border trade for e-commerce providers. It stated that cross-country legal differences are a complex issue but could be "*one of the largest impediments as additional costs of compliance with another country's law*" may compel South African providers to stay local.[22]

As with similar sections, there are no specific policy options proposed in relation to cross-border trade issues. Rather stakeholders are invited to identify whether or not there are any specific mechanisms that can be put in place or particular barriers that need to be addressed to promote cross-border transactions.

- **What, if any, barriers exist in current requirements that limit cross-border transactions?**
- **What issues should South Africa be raising in regional, African and/or international forums in relation to this?**
- **Are there any policies and or amendments to the ECT Act that you propose to address barriers to cross-border trade in South Africa?**

4.5.6 SMME Development

The development of SMME's is one of the priorities set in South Africa's economic development framework. The introduction of a Ministry and Department of Small Business Development in April 2014 is a key step in facilitating growth in this area.

[21] Kommerskollegium, "E-Commerce: New opportunities, New barriers", 2012, http://www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/ecom_national_board_e.pdf
[22] PPF, Green Paper submission, page 11

Digital technologies provide opportunities for SMMEs to enter the e-commerce market and can assist in reducing start-up costs of SMMEs in other sectors by decreasing the costs of products and services (e.g. cloud computing can reduce high infrastructure costs). It is important, however, to ensure that any new entrepreneurs entering the ICT and e-commerce sectors have sufficient skills and information to protect themselves, users and potential clients from cyber threats (including protection of data, adequate anti-virus protection and tools to ensure secure networks). The Department and Ministry will work with the new Ministry and Department of Small Business Development to holistically address these issues and consider the specific skills needs of the entrepreneurial sector.

- **Stakeholders are invited to submit ideas on how the policy could support and promote SMMEs in the e-commerce sector.**
- **What challenges do SMMEs currently face?**

4.6 Cloud computing

Cloud computing involves the storing, processing and use of data on remotely located computers accessed over the Internet. The ITU defines cloud computing as:

> "A model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud computing enables cloud services."[23]

Cloud computing has the potential to lower barriers to entry for new players as it allows for government agencies, individuals, entrepreneurs, SMMEs and other companies to access IT resources on demand without significant capital expenditure. South Africa needs to ensure its policies facilitate cloud computing as a platform for innovation and job creation, promoting the development of new services and products. This should be balanced with the need to protect privacy and the security of information, data and systems. There are also issues regarding the liability of service providers (noting that these may be global) and the need to promote open standards to facilitate fair competition between service providers.

Cloud computing can also support government IT development, e-government and development services and priorities. Government is a major user of IT services, software and hardware. Innovative use of cloud computing solutions could result in significant savings for national, provincial and local government and public entities and allow for better organisation. This will require coordination at a national level to ensure that government leverages the most benefits and that common cloud standards are promoted across the public service.

Cloud computing as a tool for development is an area that should be further explored, given the potential it offers in areas such as education, health care and promotion of open government. Cloud services designed for mobile devices (including phones) are another important issue to explore further in this regard.

[23] ITU, "Cloud Computing Standards: Overview and ITU-T positioning", http://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00001C0043PDFE.pdf

Because of the nature of cloud computing, it is also critical that South Africa not only focuses on its own policies, but works together with its neighbours and with the international community to ensure that the benefits of this platform can be realised while protecting privacy, security and consumer rights. The impact of cloud services on taxation and cross-border controls will also have to be carefully considered.

The OECD in a paper on cloud computing suggested the following areas for government intervention. Many of these issues are not specific to cloud computing (e.g. taxation and protection of privacy), and are covered in other sections of this Chapter or the Discussion Paper. They are nevertheless listed for completeness:

- Raising awareness of cloud computing, developing skills and education to ensure understanding of the concept, its benefits and challenges.
- Developing intra-government policies on cloud computing.
- Promoting research and development into cloud computing solutions and open standards.
- Standardisation and the promotion of open, interoperable and appropriate standards to address potential vendor lock-in.
- Introducing mechanisms to measure cloud computing and tools to collect data on revenues, supply and demand, cross-border flows of data and the location of data.
- Focusing on building cloud computing infrastructure in South Africa in partnership with other partners (such as SADC and BRICS) to address the current unequal flow of data given that most cloud computing providers are located in the northern hemisphere.
- Addressing potential competition and trade implications that could arise if the sector is dominated by a few companies.
- Consideration of the tax implications. Cloud computing has the potential to improve standards of record-keeping by SMME's in particular but there will also be a need to have flexible policies to address future challenges that might arise (e.g. tax evasion).
- Consumer protection and a specific focus on cloud computing contracts recognising that individuals and smaller companies will not have the power to negotiate on contracts. Privacy and security are critical issues as providers may not necessarily be located in South Africa.[24]

- **Should South Africa develop a specific cloud computing policy to address these issues?**
- **How can this best be coordinated, recognising that these issues are relevant across a range of government departments and entities and to the private and non-governmental sectors?**
- **What role should the DTPS and/or the regulator play in this regard?**
- **How can open standards be promoted?**
- **What role should government play in promoting awareness and skills development?**

[24] OECD, "Cloud computing: The Concept, Impacts and the Role of Government Policy", Digital Economy Papers no 240, 19 August 2014, http://www.keepeek.com/Digital-Asset-Management/oecd/science-and-technology/cloud-computing-the-concept-impacts-and-the-role-of-government-policy_5jxzf4lcc7f5-en#page1

4.7 Internet Governance

> "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." [25]

4.7.1 International institutions

4.7.1.1 ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) has overall responsibility for managing the Domain Naming System (DNS). It administers the root domain, delegating control over each Top Level Domain (TLD) to a ccTLD administrator, such as .ZA Domain Name Authority (zaDNA). zaDNA is an active participant in the country code Name Supporting Organisation (ccNSO) of ICANN.

Government has participated in ICANN's Governmental Advisory Council (GAC). The GAC's main limitation is that it is an advisory structure, and the ICANN Board only has to consider rather than accept its advice. This status effectively means that other stakeholders have a stronger platform within ICANN to push their interests than governments. ICANN's work however entails wide-ranging public policy issues that cannot be left entirely in the hands of the private sector.

The position that governments currently occupy within ICANN is made more powerless by the fact that the US government maintains sole influence over what ICANN does and how it does it. This is contrary to agreements reached in the 2005 Tunis meeting of WSIS. The Tunis Agenda for the Information Society outlines the roles and responsibilities of all stakeholders in Internet governance and recognises that governments are custodians of public policy:

> *"*The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organisations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism. … We commit ourselves to the stability and security of the Internet as a global facility and to ensuring the requisite legitimacy of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities. *"*[26]

In the past, calls have been made by some governments to have the ITU take over the role of ICANN. This view has now apparently lost substantial support, seemingly because of the appreciation that the ITU is not suited to play such a role. South Africa's BRICS partners have in the last two years repeatedly reinforced the need for governance to be brought in line with the WSIS Tuna Agenda and have called for an enhanced role for governments within ICANN. In the recent past, the European Union has made calls to have ICANN internationalised and relocated to Geneva so that it can be seen to be really free from the US government influence.

South Africa will need to determine its own positions and participate in the debate at national, regional and international level. This may include giving governments their own structure to which ICANN accounts in public policy issues. Such a structure would have to have clear terms of reference, and be equally representative of different UN regions.

---

[25] Report of the Working Group on Internet Governance (WGIG), June 2005

[26] WSIS, "The Tunis Agenda for the Information Society", paragraphs 29-35

One of the other weaknesses in the current ICANN multi-stakeholder model is the lack of clarity regarding the definition of multi-stakeholders and the process of accepting such stakeholders in ICANN structures. Most of the exiting stakeholders are moreover largely from the developed economies, with Africa and other developing regions having little meaningful participation. This approach it has been argued will dilute the influence of developing countries, including South Africa, contrary to South Africa's general foreign policy approach to building a multilateral rules-based system which can act as a buffer to excessive influence by individual or groups of countries.

Research ICT Africa emphasised in its submission on the Green Paper that South Africa needs to adopt a "clear policy" on Internet Governance that will allow the country to "*defend its interests, its constitutional values and more actively influence global governance outcomes*".[27]

- **What positions should the South African government adopt to address challenges in the current ICANN model?**
- **How can the weaknesses identified above in the multi-stakeholder concept for Internet governance of ICANN be addressed in this policy position?**
- **What type of internet governance framework would ensure all role players are involved?**
- **What would be the best model to ensure participatory internet governance?**

4.7.1.2 Regional Internet Registries

Regional internet registries receive IP address allocations from ICANN and sell them usually to ISPs in their region. The African Network Information Centre (AfriNIC) is Africa's regional internet registry. South Africa's participation in AfriNIC is through local ISPs that are members of AfriNIC. AfriNIC is also responsible for developing and implementing policy guiding IP address in Africa.

4.7.2 South African institutions

The ECT Act established the .ZA Domain Name Authority (zaDNA) in 2002. It is responsible for the .za domain name space and is the statutory regulator of South Africa's domain name space, dotZA (.ZA). Its mandate is enshrined in Chapter X of the ECT Act which requires zaDNA to regulate and manage the namespace, including licensing registries and registrars. The ECT Act also makes provision for alternative dispute resolution mechanisms. It is a practice initiated by ICANN, which developed the Uniform Dispute Resolution Policy (UDPR). The UDPR was designed to allow trademark holders to recover domain names registered in bad faith and is based on the First WIPO Internet Domain Name Process.

To date, zaDNA has not implemented the licensing regime set out in legislation due to inadequacies in the Act. The ECT Amendment Bill published in 2012 addresses gaps in the existing legislation. The Bill, for example:

- Gives zaDNA final overall responsibility for the DNS in South Africa in recognition that there are a number of registry operators administering second-level domain names, such as UNIFORUM South Africa (.co.za), state-owned SITA (.gov.za) and privately-owned Internet Solutions (Pty) Ltd (.org.za). The Bill states that to ensure stability of the system, zaDNA must be able to perform the functions of the registrars and registry operators as and when required.

[27] Research ICT Africa, Green Paper submission, page 6

- States that to the extent that zaDNA does receive funds from National Revenue Fund or other government sources, it should be required to report on them to Parliament, but this is an obligation that need not apply to funds that zaDNA receives from other sources.
- Addresses gaps and issues relating to the appointment of the Board.
- Introduces new provisions to address the registration by ICANN of new generic domain names. This is for several reasons:
    - Domain names are becoming increasingly important.
    - South African names that are intrinsically of national importance or relevance should be treated differently than corporate or brand names for reasons of public interest.
    - It is proposed that geographic or cultural gTLDs that are uniquely South African should not be registered without the permission of the Minister. These names might include any reference to a South African national language, place name, heritage site, historical event, product or service, or a South African national team. The registration of a South African language domain name such as .zulu by a non-South African for example, would be innately wrong.

The domain name authority has proposed that any policy and legislative review further consider options in relation to regulation of registries. Currently, zaDNA regulates the ZA Central Registry through an operating agreement:

- Policy and law could allow for regulation of registries through an accreditation agreement to promote speedy responses to deal with the fast-changing and fast-developing internet.
- Policy and law could consider requiring the registries, instead of zaDNA to accredit registrars. It stated that in practice the real interface with registrars lies primarily with the registries and not zaDNA. The ZACR already has +400 accredited registrars for .ZA, and also has to interface with +1000 international ICANN-accredited registrars because it operates the dotAfrica, dotCapeTown, dotDurban and dotJoburg domains.

  zaDNA stated that leaving registrar accreditation to the ZACR may enable the ZACR to better adapt its systems to deal with registrars using two autonomous regulatory frameworks (i.e. the .ZA framework based on SA law, and the ICANN framework based on US law).

  The domain name authority noted that having zaDNA continuing to be responsible for accrediting/licensing the .ZA registrars is not necessarily unsustainable. Australia (.au) accredits both registries and registrars, and has not reported any problems with this approach. In New Zealand, InternetNZ has a Domain Name Commission that accredits the registry operator – NZ Registry Services – and the NZ registrars.

Cell C in its submission on the Green Paper recommended that the ICT Policy Review process should benchmark best practice in other countries. This should include the relationship between the domain authority and ICASA and their differing responsibilities.

POLICY OPTIONS: LICENSING VERSUS ACCREDITATION

Option One: Status quo

zaDNA continues to be responsible for licensing (rather than accrediting) registries once the necessary amendments to the ECT Act have been finalised.

Option Two: Accreditation allowed

The policy and law provide for zaDNA to accredit registries and set rules in relation to this.

- **Please select your preferred option. Please motivate and elaborate on specific policy and/or legislative provisions you suggest in relation to your preferred option.**

POLICY OPTIONS: RESPONSIBILITY FOR ACCREDITING REGISTRARS

Option One: Status quo

The status quo remains and zaDNA remains responsible for accrediting .ZA registrars.

Option Two: Registries responsible for accreditation of .ZA registrars

The policy and law could give responsibility for accreditation of .ZA registrars to licensed/accredited registries (see above).

- **Please select your preferred option and state why you prefer this approach.**
- **Are there any other proposals or amendments that you believe would strengthen the existing registration process?**

4.7.3 Domain names and mandate of zaDNA

South Africa's authority in domain names only applies to the names registered in .ZA, and zaDNA is the entity entrusted with this authority. Domain names registered in other namespaces do not fall under its jurisdiction. Each country in the internet governance environment retains autonomy over how it runs and regulates its internet namespace. Generic top level domains (gTLDs) such as .com, .net and .org do not identify a specific country but are open to domain name registrations from entities around the world. All gTLDs (including the around 1300 new gTLDs added since 2013) fall under the jurisdiction of the US government simply because gTLDs account to ICANN, which is a California-registered entity.

There are currently just under one million names registered in South Africa to date (.ZA domain names). This is limited given that the population of South Africa is +50 million people, and can, at least in part, be linked to the broader socio-economic realities of South Africa where a substantial percentage of the population do not have Internet access. Domain names have further not formed part of broader ICT service delivery, due largely to lack of domain name education and awareness.

Another factor is that the internet is global, and there is nothing that hinders South Africans from registering domain names elsewhere (e.g. in .com and .net). A survey conducted by ZADNA in 2010 showed that domain names registered in namespaces other than .ZA accounted for almost 20% of all registered domain names in the country. This figure is likely to have dropped slightly because .ZA awareness, especially in the local registrar community, has grown substantially in the last five years.

zaDNA suggested in its submissions that its mandate could be extended to cover broad Internet awareness beyond just domain name awareness. The ECT Act currently states that it must enhance public awareness on the economic and commercial benefits of domain name registration (section 65(2)). The policy could stipulate that zaDNA should develop and implement strategies to ensure a more forward-looking Internet policy and generally promote Internet awareness and security. It could also be specifically mandated to develop proposals on ICT technical skills training at primary and tertiary institutions and, for example, engage with FET colleges to develop technical course

certification relating to Internet standards and domain names. Such capacity building could include a focus on enterprise development and the establishment of registrar and hosting businesses in order to take advantage of the opportunities that come with the expansion of the domain name landscape There are several models in other countries of internet authorities that have such a wider mandate, including in China and Korea.

POLICY OPTIONS: ZADNA MANDATE

Option One: zaDNA's mandate is extended

zaDNA's mandate could be extended to cover awareness raising of all Internet related issues and develop and implement strategies to extend South Africa's presence on the Internet. It could further be tasked with engaging with educational authorities to extend training on Internet governance and domain name hosting.
If this is your preferred option, please detail what specific issues you think ZADNA should be given additional responsibility for.

Option Two: Status quo

zaDNA's mandate would focus on increasing public awareness on the economic and commercial benefits of domain name registration.

- **Please select your preferred option.**

4.7.4 Domain name security

Issues of domain name security relate largely to security and reliability of both the domain name registry infrastructure and the integrity of domain name data. There are a range of different security measures that domain name regulators have used in the past to secure their namespaces, though ICANN – as the "regulator" of all generic, non-country specific top level domains – has required that registry operators implement DNS Security (DNSSec). The Internet Society (internetsociety.org) explains DNSSec as follows:

> *"DNS Security (DNSSEC) is designed to authenticate DNS response data. It verifies responses to ensure a DNS server's response is what the zone administrator intended. It does not address all threats (nothing does), but it provides a building block for providing additional data security, and not just within the DNS but also within the applications and services that are built on it."*[28]

DNSSec is gradually gaining momentum in line with this ICANN requirement and an increasing number of country-specific domain name regulators are now implementing DNSSec. In South Africa, ZADNA has committed to a gradual DNSSec deployment starting in the near future.

POLICY OPTIONS

As ZADNA has already identified DNSSec as a value-adding security measure for the .ZA namespace, it is proposed that this be endorsed in policy.

[28] http://www.internetsociety.org/deploy360/dnssec/

4.7.5 Dispute resolution

The ECT Act states that the Minister together with the Minister of Trade and Industry must promulgate regulations on the resolution of disputes in the .za domain name space (section 69). Regulations were promulgated in 2007 (the Domain Name Dispute Resolution Regulations).[29]

In the subsequent seven years of domain name dispute resolution practice some trends and uncertainties have surfaced that necessitate a review of the Regulations. These include:

- The need to consider including provisions allowing for the deletion or cancellation of a domain name in order to avoid the rights of third parties being ignored.
- The need to extend the list of factors which may be evidence that a domain name is an abusive registration. Regulations could further clarify the term abusive registration to avoid too rigid application. It could, for example, add provisions similar to those in the UK rules:
    - The regulations could clearly state that the failure on the part of the registrant to use the domain name for the purposes of email or a website is not in itself evidence of an abusive registration.[30]
    - They could make it clear that domain name practices such as trading domain names for profit and holding large portfolios of domain names are not as such objectionable activities.
- Suggestions that the initiation of an informal mediation procedure should be mandatory.
- The issue of 'reverse domain name hijacking' (when a trademark owner attempts to secure a domain name by making false cybersquatting claims against a domain name's rightful owner) could be more thoroughly addressed. Reverse domain name hijacking is most often perpetuated by larger corporations against smaller organisations or individuals.[31] In the US some legal professionals have proposed that laws should specifically facilitate litigation against reverse cyber-squatters and introduce severe penalties to deter such actions.

- Is there a need to review ECT Act provisions on the promulgation of regulations to ensure that the process is efficient? If so, what amendments do you propose to address this?
- Is there a need to include in policy and/or legislation clear definitions of prohibited practices (such as abusive practices and domain name hijacking)?
- How could the dispute resolution provisions be strengthened?

4.8 Ensuring trust and confidence in the Internet

Public and business trust and confidence in the Internet is essential to promote both e-government and e-commerce services. There are a number of issues which need to be addressed linked to this:

- Mechanisms to address cybercrime and protect users from criminal activity on the Internet or via their mobile phones (e.g. SIM swaps);
- Enhanced tools to deal with cybersecurity;
- Ensuring that data is protected;
- Provisions to ensure privacy of users;
- Consumer protection;
- The protection of children; and
- Intellectual property protection.

[29] http://www.domaindisputes.co.za/downloads/AFTLDPresentation.pdf
[30] Nominet 'Dispute Resolution Service Policy'
[31] Sallen v. Corinthians Licenciamentos Ltda., 2002 U.S. Dist. LEXIS 19976 (D. Mass. Dec. 19, 2000), rev'd, 273 F.3d 14, 17 (1st Cir. 2001)

Promoting awareness of mechanisms and tools to protect end-users (digital literacy, e-awareness etc.) is part of this, but is dealt with in its own section as there are many dimensions to this.

4.8.1 Cybersecurity

The National Cybersecurity Policy Framework adopted by Cabinet in 2012 defines cybersecurity as follows:

> *"**Cybersecurity** is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user assets."*

Government recognises that the issue of cybersecurity is cross-cutting and cannot be addressed by one department alone. In line with this, the Cabinet Justice, Crime Prevention and Security Cluster (JCPS Cluster), led by the Minister of Justice, is currently reviewing all related legislation to ensure harmonisation and alignment. The DTPS is part of the Cyber Response Committee (CRC) established under the Cluster and is thus integrally involved in ensuring alignment with the ECT Act. The State Security Agency is tasked with the overall responsibility of cybersecurity and is working together with other relevant departments on this, including DTPS.

It is noted that the MPDP in its submission to the Green Paper proposed that the DTPS be responsible for cybersecurity rather than the Department of State Security. It argued that there is insufficient evidence to show that State Security is under threat and proposed that the issue should be dealt with "*principally through an information security framework and strategy*"[32].

The NCAC however asked why the Green Paper even raised questions on cybersecurity as this it stated is a matter for the Department of State Security and the JCPS Cluster. It stated that there have been delays in implementation of policy and urged that Government "*advance with speed*". It raised concern that the Policy remains a classified document and stated that Government should realise it is crucial that a public version is developed "*since this is part of building confidence in the secure use of ICTs in the country*".[33]

Intel agreed generally with the NCAC and included in its submission draft cybersecurity guidelines which could be considered. It also highlighted the importance of ensuring that cybersecurity policy should be technology neutral and focus on "*normative business process and risk management processes rather than prescriptive technology solutions*".[34] The South African Chamber of Commerce and Industry (SACCI) agreed that policies must technology-neutral and innovation friendly. It stressed that there is a need for dynamic information sharing between the public and private sectors, focused on addressing specific challenges and responding to specific threats. [35]

Vodacom stated that the definition of what constitutes cybersecurity threats needs to be expanded to include critical infrastructure such as electricity, given the impact of outages on services. It stated that a cybersecurity policy incorporate incentives to facilitate the widespread adoption of

[32] MPDP, Green Paper submission, page 25
[33] NCAC, Green Paper submission, page 6
[34] Intel Corporation, Green Paper submission, pages 35-38
[35] SACCI, Green Paper submission, page 6

cybersecurity measures across all sectors. This it proposed should be led by the Presidency and should promote active local and international partnerships to facilitate exchanges of information. [36]

It should be noted that one of the core mandates of the Cybersecurity Hub (see below) is to promote awareness of risks and vulnerabilities.

PROPOSAL

Government has acknowledged the need to benchmark cybersecurity related frameworks, policies and laws in terms of international best practice, taking into consideration the need to promote security while protecting rights encapsulated in the Bill of Rights. A cross-ministerial Cluster is taking responsibility of this.

- **How, if at all, could this approach could be strengthened?**

4.8.2 Cybersecurity hub

The National Cybersecurity Policy Framework mandates the DTPS to establish a National Cybersecurity Hub. This is in the process of being implemented. Provisions relating to this have been incorporated into the ECT Amendment Bill which proposes that the Hub:

- Is the national point of contact for the coordination of cybersecurity incident handling activities,
- Identifies stakeholders, develops public-private relationships and collaborates with sector Computer Security Incident Response Teams (CSIRTs) to centralise coordination for cybersecurity issues and enable organisations to overcome the barriers and differences between languages, security cultures, laws, regulations and time zones.
- Facilitates interaction, both nationally and internationally, including through international memberships to organisations such as the Forum for Incident Response and Security Teams (FIRST); and
- Coordinates the promotion of cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) to address cybersecurity threats.

The Policy Framework also proposes the establishment of a Government CSIRT and promotes the establishment of Sector CSIRTs to manage the operational aspects of cybersecurity.

Vodacom suggested that the government established response team should also be responsible for collecting and publishing statistics on cyber-attacks, the different types of attacks, responses to these and mechanisms to be put in place to prevent reoccurrence. It should be a "single point-of-contact" and coordinate CERTs already in place in individual sectors. It said that international experience showed that cybersecurity issues are best placed in the Presidency and that the Security Agency is the most appropriate agency to take responsibility for CERTs.[37]

The NCAC also raised the issue of reliable statistics stating that it is critical that such statistics are collected in order to have a "*South African view of the risks rather than depend on international statistics*". It asked further if cybercrime reporting could be made a legal requirement.[38]

[36] Vodacom, Green Paper Submission, page 38
[37] Vodacom, Green Paper Submission, page 38
[38] NCAC, Green Paper submission, page 16

MTN proposed that skills development in relation to cybercrime and cybersecurity become a further focus area for the Cybersecurity Hub. The mobile operator further proposed that the Hub be required to enter into MoUs with relevant law enforcement agencies, the Companies and Intellectual Property Commission and the private sector to address "*mutual assistance and co-operation in respect of the identification, investigation and prosecution of cybercrime and the related offenses at a national level, utilising the existing legal framework*". [39]

POLICY PROPOSALS

The DTPS has established the Cybersecurity Hub in line with the National Framework. It is recognised that there is a need for strong public-private partnerships and that it might be necessary to develop an enforceable code of conduct and legal rules to incentivise implementation across government and society of good cybersecurity practices and address liability for cyber breaches such as identity theft and/or cyber financial theft. For example, private parties might be more likely to invest in cybersecurity if they must also bear some of the cost of cybersecurity failures.

- **Is the mandate for the Cybersecurity Hub provided for in the ECT Amendment Bill appropriate?**
- **How, if at all, could provisions be strengthened?**
- **How do you propose policy and legislation address the issue of liability for cyber breaches?**

4.8.3 Critical databases/critical information infrastructure

The protection of critical information databases has been prioritised in the National Cybersecurity Framework. The Cyber Response Committee (CRC) established under the JCPS Cluster has developed a draft National Critical Information Infrastructure Policy outlining an approach to the identification, protection and security of the national information infrastructure. The draft policy categorises such infrastructure as that which is "*critical for the provisioning of essential services to South Africans".*[40] The ECT Act and the Amendment Bill will be adjusted if necessary to accommodate approaches and policies identified in the policy once this has been adopted.

The ECT Act states that the Minister is responsible for developing standards and regulations identifying which classes of information are of importance to "*the protection of the national security of the Republic or the economic or social well-being of its citizens*" as well as prescribing rules for the registration, management and protection of such databases (sections 52-58). The 2012 Amendment Bill includes several amendments to this focused on broadening related provisions to focus on **critical information and critical information infrastructure** rather than just **critical data and critical databases**. The term 'critical information infrastructure' is defined as "*a collection of critical information that is stored or conveyed in or converted to electronic form within an electronic communications network from which it may be accessed, reproduced, distributed or extracted*".[41] Given this proposed amendment, the terms infrastructure and databases and data and information are used together in this text.

[39] MTN, Green Paper submission, pages 26-28
[40] South African Government, "Minister Nathi Nhleko: Justice, Crime Prevention and Security Cluster media briefing", 30 October 2014, http://www.gov.za/minister-nathi-nhleko-justice-crime-prevention-and-security-cluster-media-briefing
[41] ECT Amendment Bill, Section 1: Amendment of Section 1 of Act 36 of 2002

Section 53 of the Act states that the Minister may gazette which classes of information are of "*importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data [information]*" and that s/he must "*establish procedures to be followed in the identification of [national] critical databases [information infrastructure]*". The legislation states that the Minister may set out requirements for registration of national or other critical databases/information infrastructure with the Department as well as minimum standards or prohibitions in relation to the general management, storage and disaster recovery plans of such databases/infrastructure and rules for securing the "*integrity and authenticity*" of critical information. These standards must be set in consultation with all members of Cabinet.

Several submissions focused on this issue.

The NCAC highlighted that concerns were raised in the development of the Act about the appropriateness of the Department being responsible for critical databases, but it said these were ignored. The Advisory Council also raised a concern that the related provisions have never been properly acted on. It proposed that the provisions be reviewed, that the issue of where protection of critical databases is located is again debated and that any provisions facilitate partnerships with the private sector as much of the technology critical to both cyber and national security is not owned by Government. The Council stated that the current wording is prescriptive and limits such partnerships.[42]

The SACF raised additional concerns, stating that the relevant sections are too vague and therefore potentially over-reaching. They emphasised that the current provisions give the Minister "*unfettered discretion*" to determine what is critical data/information and critical information databases/infrastructure.
The Intel Corporation proposed that policy should limit the regulatory framework to "*vital cyber-physical systems that control core critical infrastructure and whose failure would result in mass casualties, a significant national security incident or a catastrophic halt of economic markets*". It stated that an overly broad scope could capture "*many unnecessary elements of the Internet economy and its customers spread resources too thin and defer or delay other investment decisions related to security*". Other entities it said could be governed by voluntary codes of conduct.[43]

POLICY OPTIONS: RESPONSIBILITY

Policy option one: Status quo

The Minister would remain responsible for setting rules and overseeing the management of critical information infrastructure. Amendments could be made to policy and legislation if necessary to address gaps (if any) in current provisions.

Policy option two: The responsibility is given to another Ministry

The responsibility would be given to another Ministry under the JCPS Cluster.

[42] NCAC, Green Paper submission, pages 6-9
[43] Intel Corporation, Green Paper submission, pages 37-38

POLICY OPTIONS: AMBIT

Policy option One: Status quo

The definition would remain broad giving the responsible Minister the power to define what classes of information will be regarded as critical information and which information infrastructure will be included.

Policy option Two: Limit to state owned critical information and infrastructure

The terms critical information and critical information infrastructure would be clearly defined to limit the Minister's powers in this regard.
In responding to this question, stakeholders should note that it is difficult to isolate state-owned information infrastructure due to the connectivity of networks. The issue of protecting infrastructure is not about government vs. private sector, but about ensuring the safety and security of South Africa. It is recognised that there needs to be a holistic approach to protecting critical information infrastructure and, as highlighted by some stakeholders, it should be recognised that much of the critical information infrastructure is owned by private entities.

- **Which options do you prefer in relation to the above policy proposals?**
- How could self-regulation and the development of voluntary codes be supported in policy and legislation**?**

4.8.4 Cybercrime

Cybercrime is an increasing concern in South Africa and around the world. It affects public entities, individuals, community and non-governmental organisations as well as private enterprises. The ECT Act currently deals to some extent with cybercrime related issues and, for example, includes penalties for such crimes. A Cybercrime Policy is currently being developed by the SAPS together with the JCPS Cluster.

Several submissions said that current provisions in the ECT Act are inadequate (e.g. the penalties provided for crimes are too low) and proposed that issues relating to cybercrime be removed and dealt with by the Justice and related Ministries (including the police) to ensure proper deterrents, and provide for investigation, prosecution and enforcement of provisions.[44]

The NCAC noted that *"with very few exceptions, law enforcement is ill-equipped, prosecutors do not understand the law and presiding officers in legal proceedings do not have sufficient background or experience in ICT issues to enforce the law*". It said that given this, "*it is not at all surprising that cyber criminals are able to flaunt the law with relative impunity*". Vodacom however stated that "*the fact that cybercrime is prosecuted under general criminal law means that it is difficult to prioritise it above other crimes with similar classifications (i.e. fraud, theft, etc.)"*[45]. The mobile operator suggested that best practice models could be developed which could be adapted to allow for economies of scale so that they are relevant to big enterprises, SMME's and individuals.

[44] This includes ISPA and the NCAC
[45] Vodacom, Green Paper submission, page 37

Snail attorneys proposed further that government focus on addressing current challenges in the justice system by introducing e-justice systems to streamline administration. This it stated would address delays in prosecuting crimes and ensure crime dockets are not lost or misplaced. This should include introduction of e-filing of documents/pleadings in cases to reduce administrative bureaucracy.[46]

The information above is for noting. Once a Cybercrime Policy is finalised by Cabinet, the ECT Act will be amended to ensure alignment. Submissions by stakeholders, if any, in relation to this will be shared with the JCPS Cluster and relevant Ministries.

4.8.4.1 Identity theft

Identity theft is a crime and will be addressed in any cybercrime related legislation. Individuals are often targeted in identity theft incidents. Addressing identity theft and promoting awareness of this crime is an area which could be enhanced through partnerships with the private and non-governmental sector and via self-regulation and co-regulation. Even if a cybercrime law is promulgated, it might be necessary therefore to include provisions relating to this in legislation outlining the responsibilities of ICASA. For example, licensees could be required through guidelines and/or regulations to address this issue.

ISPA in its submission indicated that it has established a voluntary self-regulatory code on protection. The 'icode project' was initiated in 2013 and "*is an industry-driven initiative to identify infected machines, inform affected consumers that they may be at risk, provide support to enable those consumers to disinfect their machines, and reduce their risk of re-infection*". It stressed that "*no component of the icode involves the interception of private communications or the inspection of any consumer's private data" and that potentially infected machines are identified through analysis of traffic patterns. It rather offers "some protection to consumers from potential identity theft due to compromised machines*".[47]

4.8.5 Cyber Inspectors

The ECT Act makes provision for the introduction of a cyber inspectorate and cyber inspectors to assist police in handling cybercrimes given the increase in cyber offences. The cyber inspectorate is a unit in the DTPS' ICT Security Directorate in the ICT Infrastructure Branch.

The inspectorate is still not fully established. Two years ago, the Department embarked on training of the first cyber inspectors. The project was not successful due to financial constraints and other administrative challenges within the Department. There are thus no cyber inspectors and no indication that the cyber inspectorate in the DTPS will be established soon.

Some aspects of the ECT Act have however been implemented. It stipulates, for example, that an internal operational procedure for the inspectorate should be developed. This has been accomplished and approved by law enforcement agencies. The ECT Act also mandates the Inspectorate to develop conditions of assistance - a guide on how the police will be assisted where necessary by cyber inspectors. The first draft has been developed pending consultation and legal input.

[46] Snail Attorneys, Green Paper submission, pages 2 & 4
[47] See www.icode.org.za

The DTPS recognises that some of the cyber inspector powers provided for in the Act overlap with those of law enforcement officers. This was highlighted in some of the submissions on the Green Paper and stakeholders proposed that these responsibilities be removed from the ECT Act and placed under the Minister of Police or other appropriate Ministry. It is noted that there is general agreement that the introduction of cyber inspectors is critical. The question is rather where it should be located.

The DTPS is of the preliminary view that an inspectorate within the DTPS is still critical considering the increasing numbers of cyber offences and the volume of work the SAPS currently handles. It is though crucial that the roles and responsibilities of any unit established under the DTPS and those of the SAPS are aligned. It is envisaged that the inspectorate would provide assistance to the police and that its powers should be confined to monitoring, investigating and inspecting websites for illicit activities and informing law enforcement agencies. This would require changes to the ECT Act and for example clauses giving inspectors the powers of search and seizure should be removed (section 82(1)).

Note that the ECT Act will be amended in line with a new Cybercrime Policy being developed by the Justice Department. Any submissions made on the roles and responsibilities of cyber inspectors and the SAPS will be shared with the JCPS Cluster and considered in finalising related policies.

Comments are invited on the proposals above on the role of the cyber inspectorate and its continued location within the DTPS.

4.8.6 Data protection and privacy

Data protection policies generally have to balance two goals: The protection of the right to privacy and promoting the free flow of data to support innovation and economic development. The information society is by its nature global and data is the currency of the digital economy. Innovations such as cloud computing, big data and the internet of things promote and rely on cross-border data flows, and South Africa needs, if it is to become more competitive, to encourage technology, business model and service innovation in this area. This, however, must not be at the expense of rights such as privacy or other goals including the promotion of SMMEs.

The Protection of Personal Information Act (the POPI Act) promulgated in 2013 deals with the issue of privacy in the processing of information and establishes an Information Protection Regulator to handle complaints. Processing includes collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, use, dissemination or merging of data. In terms of the Act, it must be done lawfully and in a reasonable manner that does not infringe the privacy of the person whose personal information is being processed. The Act requires that an entity (whether public or private) that processes personal information must notify any person if there have been any breaches of security in protection of such information. It prohibits the processing of personal information for the purpose of direct marketing unless there is consent. This is in essence requires that a person must "*opt-in*" – i.e. give express consent to use of their personal information.

The POPI Act repealed Chapter 8 of the ECT Act which dealt with the protection of personal information. The ECT Act though does still include provisions on unsolicited commercial communications which need to be reviewed in light of the new legislation. Section 45 of the ECT Act

states that a person who sends unsolicited commercial communications to any person/entity must give that person or entity an option to be removed from the mailing list and should provide on request information on where the company obtained their personal information. This is essentially an "*opt-out*" scheme. The Consumer Protection and National Credit Acts have some related provisions as well.

Numerous submissions were made on this issue.

The NCAC raised a concern that the data protection provisions in the ECT Act are voluntary in nature. It stated that these had subsequently been overridden by the Protection of Personal Information Act (POPI) and urged government to urgently begin implementing this Act and amend the ECT Act in line with this. The Council also highlighted that there is already a need to review some of the provisions in the POPI Act to strengthen the protection of privacy in line with international best practice. [48]

Microsoft emphasised that consumers continue to have real concerns about online privacy:

> *"When consumers surf the web and use online services, they often leave behind a digital data trail. While these digital data can be and frequently are used for highly beneficial purposes, they also can be misused, especially where the data is collected, processed, or exploited without the consumer's knowledge or consent. Ensuring that consumers have confidence that their private information is not being misused when they go online is essential to building trust in e-commerce—and to spurring ICT industry growth more broadly."*

Several stakeholders raised a concern about possible interpretation of clauses in the POPI Act linked to data protection and stated that it is important that instead of restricting data to a particular geography, South Africa achieves its goal of protecting user data by requiring data exporters to be accountable for the protection of that data regardless of its location. They stated that while they interpreted the POPI Act to provide for this, there is a need to clarify provisions and develop a need for a clear regulatory framework in relation to data protection.[49]

The R2K proposed that a clear policy that protects end-users' rights from corporate and government surveillance via ICTs is developed. It alleged that there has been "*a dramatic increase in the use of formal communications surveillance through RICA*". It said that it has problems with RICA as it requires that surveillance capacity be built into mobile devices and that it has no protection against the surveillance of foreign signals. It proposed that the policy and law require ICASA to develop regulations "*that protects citizens from state security overreach in ICT use*".

Note that as highlighted in Chapter Five (Policy Options: Audio and Audio-visual Content Services), the introduction of connected televisions might raise new considerations regarding privacy. In some international countries, it has been found that viewers of television-like content provided over the Internet expect greater privacy than when engaging in other activities on the web. It is also recognised that the analysis of such patterns through data trails could make it easier for on-demand providers to suggest content a viewer might like and make the selection of programming easier. In light of this, some countries have proposed that on-demand providers should explicitly spell out the

[48] NCAC, Green Paper submission, pages 8&9

[49] This included Microsoft, the PPF, the South African Chamber of Commerce and Industry (SACCI), the Information Technology Association of South Africa (ITASA)and ISPA among others

implications of data trails and provide up-front choices allowing users to "opt-out" of such schemes.[50]

POLICY OPTION: ALIGNMENT OF LAWS

Policy Option: Amendment of legislation

The ECT Act provisions on privacy and data protection will be amended to bring these in line with the POPI Act. It is also necessary to ensure alignment and coordination between ICASA and the Information Protection Regulator established under the POPI Act.

- **Are there additional provisions in the ECT Act that should be reviewed/revoked in the ECT Act to bring it in line with the POPI Act? Note that Chapter 8 has been repealed.**
- **Is there a need to consider amending provisions allowing users to "opt-out" to bring them in line with POPI Act rules requiring that consumers specifically "opt-in"?**

POLICY OPTIONS: OTHER PRIVACY ISSUES

In addition to the above broad review of the ECT Act in relation to the POPI Act, there is a need to consider whether or not current legislation (including these two laws) does address privacy and data protection sufficiently given new technological capacities. These include consideration of issues such as the right to be forgotten (as introduced in Europe) and rules on the monitoring and use of cookies by web-sites to track user's activities online.

Policy option: The right to be forgotten

The European Commission has developed a European Data Protection Regulation which includes specific provision on the right to be forgotten. In line with this, the European Court of Justice ruled against Google in May 2014 in a case brought by a Spanish man who requested the removal of a link to a digitised 1998 article online regarding a debt he had subsequently paid. The court ruled that search engines are responsible for the content they point to and thus, Google was required to comply with EU data privacy laws. [51]

- **Is there a need to provide for the right to be forgotten in South Africa? If so, is there any role that ICASA and/or the DTPS should play in entrenching this?**

Policy Option: Data trails

All Internet users leave digital trails through their Internet activities allowing for local and international entities to track and collect data about their friendship and business networks, hobbies, interests and shopping patterns. Some of the information gathered in this way is used to collect information on general trends, and is not linked therefore to a specific person. Other information gathered records a person's preferences in order to make a user's online experience more relevant (such as remembering previous music preferences on an online music site). Such information however can also be used to invade a person's privacy, or target a user with spam and

[50] This issue is under discussion in the European Union review of policies relating to audio-visual media in light of convergence

[51] Ioannis Iglezakis, "Digital Forgetting in the Age of Social Media: Establishing a Comprehensive Right to Cyber-Oblivion", http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

unsolicited emails and marketing information. Many sites include settings so that users can control their privacy settings (e.g. privacy settings on Facebook). Digital literacy and awareness programmes can assist in ensuring users are aware of ways they can protect themselves.

Privacy concerns relating to the compiling of information on a user's long-term browsing history (tracking) have prompted the European Union to introduce new rules to regulate this. The EU has introduced data protection regulation to protect Internet users from clandestine tracking and unauthorised personal data storage by requiring that "*explicit consent*" must be gathered from web users who are being tracked via web files called "*cookies*".[52] The definition of personal data includes any information online that can be traced to an individual. More stringent rules on the online profiling of children are included.[53]

In 1998, the USA introduced a law specifically limiting tracking of children's online activity – the Children's Online Privacy Protection Rule. The Federal Trade Commission is responsible for enforcing this.[54] The California State Government in the USA has recently introduced a law requiring disclosure from websites about their tracking of consumers' behaviour.

Given the global nature of the Internet, it is important that any rules are aligned and there have been suggestions that a global privacy policy should be adopted by an international body.

Currently both the POPI and ECT Acts include provisions on privacy in relation to unsolicited marketing.

- **Is there a need to introduce specific policies and rules regarding online privacy in South Africa? Please motivate your response and indicate what, if any, policies and rules you propose.**
- **Is there a need to strengthen rules in place regarding the protection of children's privacy online? Please motivate your response and indicate what policies and rules you propose.**
- **What role could the DTPS and/or ICASA play in relation to ensuring online privacy protection?**

4.8.7 Online gambling

Increased access to the Internet (whether via computers or mobile devices) inevitably increases the reach of online casinos. Online gambling includes virtual online gaming, Internet sports betting, online bingo and online lotteries and online sweepstakes and tournaments. While the National Gambling Act, no 7 of 1996 regulates gambling activities, these online sites challenge the effectiveness of such laws, given that online operators are not necessarily located within South Africa. The potential for fraud and cybercrime also increases as dishonest operators of sites can easily move, alter or even remove a site within minutes after taking money from gamblers. It is also easy for unscrupulous operators to manipulate software and games.

[52] BBC, "New net rules set to make cookies crumble", 8 March 2011, http://www.bbc.co.uk/news/technology-12668552
[53] European Commission, "Online privacy", https://ec.europa.eu/digital-agenda/en/online-privacy
[54] Federal Trade Commission, "Children's Online Privacy Protection Act of 1998", http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Amendments to the National Gambling Act adopted in 2008 provide for licensing of online casinos, however regulations required in relation to this have not yet been promulgated by the Gambling Board or the Department of Trade and Industry.

While this Discussion Paper, and the subsequent White Paper, will not explicitly deal with challenges associated with online gambling regulation or with the implantation of legislation, it is important to note that the failure to implement provisions and address the associated problems can result in loss of confidence among end-users who have been exploited or who are aware of such exploitation. A loss of trust inevitably negatively affects all online or mobile service providers and therefore impact on e-commerce expansion. This Discussion Paper therefore raises such issues so that they can be referred to the relevant Ministry as well as to other entities to address.

- **How could concerns around online gambling be addressed, if at all? Please indicate which entities you believe should be involved in this and their roles in addressing such challenges.**
- **Are there any rules that the DTPS or ICASA could introduce to address concerns related to online gambling?**

4.8.8 Internet intermediary liability

It is believed that a Cybercrime Bill developed by the Department of Justice, will deal with this issue to some extent. If necessary, the ECT Act might need to be amended to ensure alignment between the different laws. This would it is presumed focus on liability in relation to court actions. Given, however, that the ECT Act currently also provides for the issuing of take-down processes outside of the courts, this section considers whether or not it would be necessary to retain such provisions in an ICT policy and in legislation. It further asks questions about whether or not there is a need to amend current provisions.

Chapter XI of the ECT Act includes limitations on liability for ISPs under certain conditions. The Chapter states that intermediaries have limited liability if they are a member of an industry representative body recognised by the Minister, they conduct their operations in an automatic manner, adhere to the industry body's code of conduct and respond to court orders and take-down notices. ISPA was recognised by the Minister as an industry representative body in 2009 and therefore its members have limited liability when transmitting, caching and storing, hosting and linking or referring to unlawful content as long as the ISP is not aware of the content or did not actively create or modify this. ISPs also need as stated to participate in notice and take-down procedures outlined in Section 77 of the ECT Act.

The take-down provisions state that any person who becomes aware of unlawful material or action taking place on the network of an intermediary may notify the intermediary of the infringement and require it to remove or disable access to the material. In terms of legislation, ISPs can ignore a take-down notice if it is not valid (i.e. if it violates other laws or is in bad faith). The burden of proof of the invalidity of the notice however rests with the intermediary.

According to the ECT Act procedures "*any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down*." It also states, however, that a "*service provider is not liable for wrongful take-*

down in response to a notification." The Act does not provide for an appeals mechanism against take-down notices other than through the courts, though proposed amendments to the Act do deal with this in part. These amendments stipulate that a service provider has 10 working days to respond to a first take-down notice after which a second notice must be sent. It is not specifically stated that the creator or uploader of the allegedly infringing content should have be given a chance to respond to this notice.

Questions have been asked about whether or not any entity other than a court should be allowed to issue take-down notices.

ISPA in a supplementary submission on the Green Paper generally supported current provisions as they allow service providers to operate without "*undue legal risk*". The industry body however stated that it did have concerns regarding the take-down procedures and questioned if these constituted a "*justifiable limitation on the constitutional right to freedom of speech*" as there are no processes in place to assess the merits of any allegations informing a take-down notice. ISPA further highlighted that the largest ISPs in South Africa (the mobile networks and Telkom) are not members of any industry body recognised by the Minister in terms of the Act and noted that this could imply that common law does limit liability "*given the level of legal expertise these entities are able to access and their general risk-averse culture*".[55]
The Minister of Trade and Industry appointed a Copyright Review Commission (CRC) to consider all provisions relating to copyright in South Africa. In its 2011 report, the Commission recommended that the ECT Act and the Ministerial Guidelines for Recognition of Industry Representative Bodies of Information System Service Providers should be amended to require ISPs to adopt a graduated response for repeat infringers of copyright culminating in the suspension of access services of an individual.[56] Similar provisions introduced in laws in other countries have come under scrutiny as it is argued that terminating the internet access of an individual for a civil offence could be seen as an unjustified infringement on the right to access information.

The FPB in the meanwhile has raised a concern that the Ministerial Guidelines do not specifically reference the Film and Publications Act and that it is necessary to address this and ensure compliance by any accredited representative body.

POLICY OPTIONS

Option One: Status quo

The current provisions would be largely retained, though specific guidelines could be included clarifying the process to be followed in accrediting of self-regulatory providers. The amendments outlined in the ECT Bill could be extended to address concerns raised regarding the fairness of the existing take-down process.

Option Two: Three strikes rules introduced

[55] ISPA, Supplementary submission, 09 October 2014, page 5
[56] http://www.gov.za/sites/www.gov.za/files/CRC%20REPORT.pdf

In addition to the above, the policy and law could provide for a three strikes policy in instances of copyright as proposed by the Copyright Review Commission (see above).

- **Please indicate your preferred option. If you opt for the status quo, please indicate what amendments you propose be included. If you agree with Option Two, please expand on how you think this should be applied.**

The following questions are also relevant:

- **Do you think these provisions should be retained in the ECT Act or rather be moved to a cybercrime law?**
- **If so, which entity should be responsible for accrediting self-regulatory bodies?**
- **Is there a need to introduce other alternative dispute resolution processes in relation to disputes over the legality of content on the Internet?**

4.8.9 Intellectual Property Protection and copyright

The Minister of Trade and Industry is responsible for the protection of intellectual property and copyright. The Ministry is currently reviewing legislation to ensure it accommodates new technologies and is in line with international best practice. Of particular concern in relation to the area of e-commerce and e-services is the issue of online piracy and trademark counterfeiting – including domain name counterfeiting.

It is noted that the take-down procedures outlined in the ECT Act dealt with above do also apply to alleged breaches of copyright and intellectual property. Proposals made on the three-strike rule by the Copyright Review Commission also relate directly to this and should be considered when responding to the questions below. Any submissions and proposals made by stakeholders in relation to this will be referred to Minister of Trade and Industry.

QUESTIONS:

- **What if any measures and mechanisms could be put in place to strengthen online intellectual property protection?**
- **Are there any policy provisions that should be introduced in an ICT White Paper and/or related legislation (such as the EC Act, the ECT Act and/or the ICASA Act?**

4.8.10 Consumer Protection

Chapter Seven (Policy Options: Institutional Frameworks) deals with the relationship between the National Consumer Commission and ICASA. The information below is therefore for noting and no specific options or questions are raised.

The increasing use of digital devices and technologies raises new issues in relation to consumer protection. ICASA is required to some extent to ensure protection of consumers though many of its responsibilities now fall under the National Consumer Commission. The Commission has however not fully implemented provisions relating to this.

MTN, among others, noted that the Consumer Protection Act provides sufficient mechanisms to protect consumers. It said that government should focus on "*properly resourcing regulatory bodies*

such as the National Consumer Commission to effectively address matters affecting consumers in the e-commerce environment" and therefore remove related provisions from ICT laws.[57] Vodacom raised similar concerns, stating that the framework is "*disjointed*" resulting in consumer confusion as they have to refer to three different laws (CP, ECT and POPI Acts) and work out which of three regulators they should complain to resulting in "*unnecessary jurisdictional battles*" .[58]

Others however stated that there is a need to make provision for specific protection from unsolicited marketing and highlighted that the provisions in the Consumer Protection Act (including the do-not call register) had not yet been fully implemented and that ICT related policy should therefore set specific provisions in rules and licence conditions.[59] The Wireless Application Service Providers' Association meanwhile stated that it has had success in dealing with consumer complaints raised against members. The Association proposed that the White Paper recognise the value of self-regulatory and co-regulatory codes to protect consumers.[60]

4.8.11 Protection of children

Several other Chapters/Policy Options Papers deal with the protection of children from harm and from accessing inappropriate content. The Film and Publications Act further includes specific provisions and outlaws certain content (including the use of children in pornography), while requiring other content (except for broadcasting content) be submitted where necessary for pre-classification. The FPB has stated that provisions are currently under review in order to ensure the Act better deals with online content.

In relation to e-commerce and e-services, however, there is a need to consider whether or not additional specific mechanisms should be introduced to, for example, put in place payment restrictions for under-age children (including mobile payments) and mechanisms and tools to restrict children's access to harmful goods such as tobacco, alcohol and gambling sites. This includes protection of children from inappropriate marketing of merchandise or services and the introduction of particular provisions on online profiling/tracking of children.

Mechanisms and tools which could be put in place include ensuring that, for example, violent games and inappropriate or adult material should only be made available on a verifiable order from an adult and should require a credit card, rather than automatically being added to the consumer's phone bill. Rules could also state that mechanisms should be put in place to ensure authentication of credit cards to guard against children using their parents' credit cards without authorisation. Such rules could also specify that that a personal identification number (PIN) is required online.

POLICY OPTIONS

As noted in the Chapter/Paper dealing with Institutional Frameworks, it is necessary to ensure ongoing cooperation between different regulatory bodies and ICASA. ICASA could also be required

[57] MTN, Green Paper submission, page 22
[58] Vodacom, Green Paper Submission, page 37
[59] This includes Snail Attorneys, Telkom, the SABC and the SACF
[60] WASPA, Green Paper submission, page 10

to strengthen consumer protection by, for example, facilitating co-regulation with licensees on such issues and/or introducing specific requirements in licence conditions or regulations related to this.

- **How could a White Paper on ICT-related policy strengthen provisions to protect children, if at all?**
- **How can self-regulation and co-regulation assist in this, if at all?**
- **What other mechanisms might be necessary to protect children – e.g. could ICASA be required to develop specific rules and/or licence conditions related to this?**

4.9 Awareness and capacity building

The need for e-literacy/digital awareness/media literacy campaigns is highlighted in a number of other Chapters/Policy Options Papers (including Content Services, Industry Growth and Institutional Frameworks). Skills development is a specific focus of the Chapter/Policy Options Paper on Industry Growth. It is recognised that in order to ensure confidence in the digital environment, security has to be assured. This includes training of lawyers, prosecutors and the judiciary on issues such as identity theft.

There is also a need for coordinated awareness campaigns about mechanisms and tools in place which can assist in protecting end-users, including, for example, anti-virus programmes, anti-spam programmes and parental filters available from ISPs. Several submissions highlighted that such awareness-raising should be the responsibility of government and industry and the SACF, for example, highlighted the role that industry should play in ensuring that users are informed about online privacy options.[61] Several submissions further proposed specific interventions for new users, and, for example, the Western Cape Provincial Government proposed that such training could be provided by libraries, community centres etc. and should be required by any entity receiving public funding to promote access.

The North West Provincial Government proposed that the DTPS introduce and co-ordinate a cybersecurity week or month that will ensure that citizens are well informed. Institutions which should be involved in this could include all spheres of government, and public entities such as the SAPS, SITA, the CSIR, Telkom and the SABC. Telkom in its submission suggested that specific mechanisms be put in place to allow for anonymous reporting of cybercrimes.[62]

While there is a need to promote awareness and digital literacy across a number of portfolios, and this should be coordinated, the ECT Act or related legislation could put in place specific provisions for e-transactions and online security awareness. This could include requiring ICASA to focus specifically on these issues, for example (as is the case with regulators in other countries such as the UK and Australia), and could include mechanisms to ensure that licensees and/or self-regulatory and co-regulatory bodies provide regular information to end-users in relation to this. Initiatives such as the "icode project" developed by ISPA could through recognition of self-regulatory bodies be given greater weight through such mechanisms.

- **Should the ECT, EC and/or ICASA Acts include specific provisions on awareness and e-literacy?**

[61] SACF, Green Paper submission, page 27
[62] Telkom, Green Paper submission, page 20

- **Would the introduction of a cybersecurity week or month lead by the DTPS assist in this?**
- **Are there regulatory, self-regulatory and/or co-regulatory provisions that could be introduced to strengthen enforcement?**
- **Should service providers receiving public funding to promote access (including funds from entities such as the USAF) be required to provide basic awareness training? If so, how could this be implemented?**

4.10 Overarching issues and coordination

The building of a dynamic and vibrant information society and digital economy requires coordination across a range of government departments and public entities and will be dependent on relationships and partnerships between government, the private sector, non-governmental organisations (including organisations for persons with disabilities) and civil society. A number of submissions to the Green Paper highlighted the need for increased cooperation between the different spheres and entities of government. Several noted that, although the ECT Act specifies that a national e-Strategy should have been adopted by Parliament by 2004,[63] this has yet to be finalised.

The National Cybersecurity Advisory Council (NCAC) said that progress had been hampered by "*departmental turf wars*". It stated that cybersecurity issues must be seen as a multi-department responsibility "*and harmonisation, alignment, optimisation, skills are fundamental requirements*". It proposed that a centralised policy and legislative function is established reporting to the Presidency to "*propose and advise on policy and legislative interventions and to monitor the implementation of ICT related initiatives*". It said that this structure should create a channel for communication between the government and other stakeholders such as the private sector and civil society and include representation from different sectors to facilitate this. [64]

Vodacom in its submission proposed that the Presidency be responsible for coordination of cybersecurity related issues and that there should be active engagement between public and private stakeholders. The framework should promote best practice risk management cultures and ensure compatibility with international approaches. It highlighted that the approach should be "proportionate" to avoid deterring investment in the infrastructure and services value chains.[65]

The SACF supported this and stated that the promotion of e-commerce and e-services needs a "*cross-functional government lead task force to deal with the larger complexities around e-commerce*".[66]

- **Is there a need for a centralised structure/function to coordinate digital related strategies and implementation across government?**
- **If so, where should it be located and which Department should play the lead role?**
- **What entities should sit on such a structure?**

[63] Section 5 of the ECT Act deals with the development of a national e-strategy. It states that the Minister of Communications should lead this process, in consultation with the Minister of Public Service and Administration.
[64] NCAC, Green Paper submission, page 2
[65] Vodacom, Green Paper submission, page 38-40
[66] SACF, Green Paper submission, page 28

4.11 Conclusion

- **Are there any other issues you think a policy on ICTs and convergence should address in relation to the information society, a digital economy and e-services?**
- **What benchmarks and targets could be included to ensure better monitoring of the effectiveness of policy?**