Implications of Convergence on the Regulatory Regime, e-Commerce, the Industry, and the Society at large in South Africa

Research Paper to Inform the Policy Process on Challenges Imposed by Convergence on Cyber Trade; e-Commerce; the Society; and the Regulatory Regime in South Africa, and Sought Solutions.

Submitted by Nhlanhla Mlitwa, bridges.org, to the Link Centre -Wits University
in Partial fulfilment of the Telecommunications Policy, Regulation, and Management (TPRM) Course

09 June 2004

Executive Summary

Convergence in information communication technology is about real issues of technological innovations and change. It encompasses a combination of benefits and challenges, not only for the market, the industry, or technology sectors, but also for the regulatory regime and the society at large.

Technology convergence offers massive opportunities for the development of new services and the expansion of consumer choice. It certainly expands the overall information market, and is the catalyst for the next stage in the integration of the world economy. Even small business can market globally, thanks to the low cost of a World Wide Web site. Convergence enables a substantially higher capacity of traditionally distinct voice and data transmission services to be transported over similar networks and to use integrated consumer devices for purposes such as telephony, television or personal computing (PC).

With these benefits however, emerges new policy and regulatory challenges, ranging from: setting manufacturing standards; cyber-trade; controlling emerging cyber-crime; protecting consumer interests, protecting intellectual property rights, and other public issues.

Different nations and institutions are applying various measures and changes in their policies, regulations, and institutional frameworks to meet new convergence related challenges. OECD countries and the EU are updating regulatory frameworks to match new industry, market, and public protection issues brought about by converging technologies. Attempts are also made to integrate national regulatory practices to match international agreements, and for governing institutions to be compatible with convergence practices.

Convergence however, is more than just a regulator issue. It extends to all policies that relate to e-commerce, manufacturing, and cyber trade, as regulated by different government departments. In SA, these policies include the Interception and monitoring Bill of the Department of Justice, the general Competition Act of the Department of Trade and Industry, and the Electronic Communications and Transactions (ECT) Bill of the Department of Communications. They regulate sectors of converging technologies, yet are implemented and enforced by different institutions, with very little national debate on how they would enable convergence.

Convergence of few laws upon which a regulator derives its mandate in SA may not adequately enable effective regulation under convergence without coherence in cross-sector policies.
This could be made possible, first, by a deliberate process of national policy debate on the coordination of convergence related policies and regulations. Secondly, by the integration of related contents among different policies directly related to convergence regulation. The ECT Bill attempts to improve the regulation of cyber-trade, interactions in electronic transactions, the industry, control of cyber crime, and the protection of consumer interest. It also provides for the formulation of a coherent national e-strategy.

However, there are evident shortfalls in the manner in which the ECT Bill attempts to address most convergence issues:

- ⇒ Providing for the formulation of the national electronic transactions policy is important. But limiting its consultation process only to cabinet and other ministers of relevant departments, instead of a broader national consultative process, and not mentioning that the future policy should address convergence issues may limit the debate, and eventually the contents of the proposed new policy.
- ⇒ While chapter III sets out legal requirements for electronic transactions, section 20 unfortunately subordinates such a provision to any other, and perhaps, even contrary regulations.
- ⇒ Updating policies to match convergence practices is not emphasised in the ECT Bill
- ⇒ Clarity is lacking on the consultative scope of the national debate that will shape the national e-strategy. Learning from the EU consultative process that followed the 1997 Convergence Green Paper is recommended in this respect.

Table of contents

1 Introduction

The aim of this paper is to discuss the implications of the convergence phenomenon on the regulatory regimes, and on modern everyday lives – using South Africa as a country of analysis.

1.1 The meaning of convergence

As a newly evolving rather than a revolutionary concept, convergence still lacks a generic or universal definition. The term is used rather interchangeably between and within contexts of integrating technologies, services and applications, markets, policies and regulations, institutions and their functions; both within and between nations.

Convergence in information communication technology is about real issues of technological innovations and change. It encompasses a combination of benefits and challenges, not only for the market, the industry, or technology sectors, but also for the regulatory regime and the society at large.

In fact, telecommunications, information technology, and media, were separate in the past (EU Green Paper, 1997:1). Services such as broadcasting, voice telephony, and online computer services such as Internet, all operated on different networks and used different devices such as Television (TV) sets, radios, telephones and computers (ibid). They were regulated through separate laws, by different regulators, without a clear need for coherence between the laws and the way they were enforced. However, modern innovation now allows different technologies to offer overlapping services outside their traditional business sectors, on an increasing scale. This process of integration between technology networks - to provide similar, overlapping, and value added services is generally referred to as technology *Convergence* (EU Green Paper, 1997:1).

To this effect, the European Union (EU) defines convergence as *the ability of different network platforms to carry essentially similar kinds of services*, including *the coming together of consumer devices such as the telephone, television and personal computing* (PC) (EU Green Paper, 1997: Sec 1.1). Convergence, adds the Organisation for Economic Co-operation and Development (OECD), is taking place not only between technologies, but also between infrastructures, and at the content, service, and application levels (OECD, 1997:11). The term is also used on a broader scale to refer to the harmonisation of telecommunications standards, policies, and regulatory frameworks between member states of institutions such as the OECD, SADC, and the EU.

Convergence as used in this paper, extends beyond the technology context, to encompass the regulatory and policy issues. In essence then, this paper enquires the extent to which the regulatory framework is adapting, and the ECT Bill responding, to technology convergence and its challenges in SA.

1.2 Opportunities and Challenges of Convergence

Technology convergence offers massive opportunities for the development of new services and the expansion of consumer choice. Digital technology now allows both traditional and new communication services - whether voice, data, sound or pictures - to be provided over many different networks. It enables a substantially higher capacity of *traditionally distinct voice* and *data* transmission services to be transported over similar networks and to use integrated consumer devices for purposes such as telephony, television or personal computing (PC) (OECD, 1997:11). For example, while an audio message could only be transmitted between telephone networks, it can now be transmitted from the telephone via the Internet using the Voice over Internet Protocol (VoIP), to another phone or computer, at lower costs. Even written data can now be transmitted through a short message system (SMS), from the Internet into mobile phones, also at lower costs (EC Discussion paper, 1998). Convergence certainly expands the overall information market, and is becoming the catalyst for the next stage in the integration of the world economy. *Even small business can market globally, thanks to the low cost of a World Wide Web site (EU Green Paper, 1997:1).*

Finally, being able to use just a PC - to send and receive a fax, an SMS, to watch videos, to play music and games, to hold a telephone conversation, and to access the Internet, all in one device, is

cost effective and convenient, both for home and work use. Along with these benefits however, emerges new policy and regulatory challenges, ranging from: *setting manufacturing standards; cyber-trade; controlling emerging cyber-crime; protecting consumer interests, protecting intellectual property rights, and other public issues (EU Green Paper, 1997:Ch IV).*

These are policy and regulatory issues that require both policy, regulation, and its implementation to develop parallel, if not ahead of technology changes if benefits of innovation are to override costs (Link Centre, 2001). It is in this context that this paper analyses implications that converging technologies have on Cyber Trade; e-Commerce; the Society; the Regulatory Regime; and the extent to which the Electronic Commerce and Transactions (ECT) Bill addresses these implications and challenges in South Africa.

2 Regulatory and Policy Challenges: Overview of Trends in the Field

As a newly evolving phenomenon, technology convergence offers advantages of convenience, efficiency, and reduced costs to the use of new technologies and services, for all who can access it. With advantages also emerge new and systematic changes to traditional ways of regulating the manufacturing and trade in converged IT, media and telecommunications goods and services within and between countries (OECD, 1996:1-2). These changes are imposing new challenges on the regulatory regime, industry, markets, and the society at large.

Different nations and institutions are applying various measures and changes in their policies, regulations, and institutional frameworks to meet new convergence related challenges. They are:

(1) Updating regulatory frameworks to match new industry, market, and public protection issues brought about by converging technologies
(2) Integrating national regulatory practices to match International agreements
(3) Updating compatibility of governing Institutions to convergence practices
(4) Improving traditional policy-making methods to suit convergence trends

2.1 Updating regulatory frameworks to match new industry, market, and public protection issues brought about by converging technologies

Current activity in the market suggests that operators from the sectors affected by convergence are acting on the opportunities provided by technological advances to enhance their traditional services and to branch out into new activities (OECD, 1996; EUGreen Paper, 1997). Telecommunications, Media and Information Technology sectors are seeking cross-product and cross-platform development as well as cross-sector share-holding (OECD, 1997:11-12). For the regulator, this implies new *cross-product* manufacturing standards, updating methods of regulating competion, trade, intellectual property rights, licencing, security, and customer protection issues across serives and sectors.

Convergence calls for increased regulator efficiency. A traditional regulator needs to overcome own internal structural uncertainties if its efficiency is to be enhanced.

Common among traditional regulators are structural limitations to their powers, which limit their capacities and eventually, certainty in effective regulation. They often are agencies of government departments and are subjected to political interferences. As such, they lack complete political independence and flexibility to make uninterrupted[1] decisions leading to effective regulation. Effective regulation according Makhaya (2001:5), is dependant upon the political will on the part of

[1] ICASA's regulatory efficiency is sometimes nullified by the fact that its regulations should first be approved by the government, who sometimes take forever to make such approvals. This sometimes leads to disputes between the regulator and industry operators. For example, the dispute between Telkom and the regulator over tariffs *…resulted from a delay by the minister in approving new tariff regulations by the Independent Communications Authority of SA (ICASA). Telkom exploited the gap, bypassed the regulations, and raised telephone costs by over 50 percent for some services (CT Business Report, May 27, 2002:1).*

the relevant ministry - to creating a strong regulatory agency. A lack of political will, as has been the case in Ghana where the government delayed staff appointments and budget allocations, argues Makhaya (2001:5), can undermine the capabilities of the regulator.

The relationship between the ministry and the regulator should be mutually supportive if the regulator is to be effective. This environment is also questionable in SA. The following statement by the Independent Communications Authority of South Africa (ICASA) chief, Mandla Langa, in describing the government and Telkom's interference with the regulator, supports this claim: "*…they (Telkom) are putting pressure on the government…to encourage ICASA to withdraw the regulations"*. However, …*ICASA does not, at the end of the day, have the final word because the minister* [Ivy Matsepe-Casaburri] *has to sign up on those regulations*" (CT Business Report, May 8, 2002: 2).

Most regulators, including ICASA, are plagued by budget constrains. ICASA for example, is struggling to hire and retain expertise of its choice. According to Langa: "*ICASA staff are lured away by operators such as MTN, Cell C, Premedia, and M-Net, who offer lucrative salaries.* Langa adds that: *"If ICASA was operating at optimum capacity, by now it would have engaged in a number of projects, including a comprehensive audit of Telkom's service roll out obligations…to put a stamp on their* [Telkom's] *assertion that they have made those targets…*"(CT Business Report, May 8, 2002: 2). Such a lack of complete financial and political independence causes uncertainty on the part of the regulator, and should be removed if the regulator efficiency is to be improved.

Further, the current lack of coherent definitions across different technologies does not help the regulator certainty. If a service that is usually delivered on a telephone is, all of a sudden, delivered over a different platform, it could be defined and regulated differently by a different regulator. For example, a voice message transmitted over the VoIP from a computer point to another computer point may not always be regarded as a phone message in all instances. This would lead to different interpretations of a technology or service by different regulators at various platforms and times. Harmonisation of definitions of converging equipments, technologies, and services could improve the regulation of standards and licensing of converging technologies and equipments.

There is a need for ICASA, as for any other regulator, to be apolitical and financially independent if a it is to improve competencies to meet the following new challenges:

(1) Licensing in converging technologies
(2) Setting of standards supporting interoperability and interconnection of converging networks, and public trusted enforcement measures
(3) Matching international standards and practices, and
(4) Balancing e-commerce and cyber trade practices with convergence trends
(EU Green Paper, 1997: Ch IV)

2.1.1 *Licensing in converging technologies*

The Telecommunications Amendment Act (2001) in SA paves the way for a number of key policy and regulatory developments expected in 2002. Chief among these is the privatisation and listing of Telkom and the licensing of a Second National Operator (SNO). Other key developments include Sentech's multimedia and international gateway licences that has come into effect, the roll-out by Telkom of ADSL, the introduction of Third Generation (3G) technology, and 1800mhz licences for the cellular companies. Watching over these developments and the hazy process of convergence is the regulator – ICASA, who has to face the challenge of regulating digital technologies that are converging at warp speed, thereby posing added difficulties for policy makers and the regulator (InfoSat News, 10 April 2002). A number of these developments involve changes in equipments, and would require relevant licensing standards by ICASA, which, of course, should be supported by an enabling policy and legislation.

While the new Act seeks to provide a consistent regulatory framework, it has gaps – such as the failure to make provision for the licensing of broadband operators, and Voice over IP. Such legislative omission limits regulator efficiency. The regulatory body, ICASA, as the InfoSat correctly observes, is already… *struggling to be effective. Under-resourced and intimidated by Telkom, the*

body is, nonetheless, doing a good job - but needs more teeth in the industry...(InfoSat news, 10 April, 2002) to be effective.

An example of licensing complexity for traditional regulation under convergence would be the case where the network meets the licensing requirements of one service regulator, and is registered as such, and turns out to offer more services including those falling under the jurisdiction of another regulator by whom it is not licensed. The second regulator would have no control of standards, and consumer protection procedures for the extra capacity. This may result into public/customer interests being endangered, with limited or no regulatory remedies.

Again here, it is recommended for regulators of similar services and networks to cooperate and integrate their regulatory efforts.

2.1.2 Setting of standards supporting interoperability and interconnection of converging networks, and public trusted enforcement measures

Convergence is heading towards the direction where a user of any ICT and infrastructure can communicate with any other user, anywhere and at anytime. While technology innovation is already making this possible, the regulatory framework is lagging behind. Current regulatory standards and practices, argues the EU, are still sector or even equipment based (EU Green Paper, 1997:Ch IV). There is still a lack of cross-product standards upon which interoperability and interconnection of services and networks can be regulated, probably because technological innovations take place daily – and faster than the regulatory practices (ibid). Such interoperability standards could further be limited by the existence of proprietary standards controlled separately by dominant players (ibid). Such a lack of standards would complicate effective regulation even further.

The open source – closed source debate, and interoperability:

> On the programming and software side, interoperability support would more likely be affected by policy decisions on the open source versus closed source debate. Convergence in this area depends largely on interoperability supporting software, yet most software is proprietary owned and hardly regulated. While ambiguity prevails within the SA policy circles on this debate, credible research continue to suggest that the open source model, relative to its closed source counterpart, builds open standards and achieves a high degree of interoperability. Largely because code re-use in open source reduces development time and *provides predictable results*. With access to the source code, the lifetime of open source software systems and their upgrades can be extended indefinitely. Proprietary source on the other hand, typically, depends on monopoly support by one company that holds access to the code for a piece of software (Kenwood, 2001: xiii; xiv). Upgrades in this regard are made only in the monopoly's terms, time, and in so far as it is economically viable for them. In that way, predictability by regulators remains limited, and regulatory processes for proprietary software remains more legally challenging. Clear policy decisions are crucial if regulator efficiency is to be enhanced over these issues in SA.

In short, there is an urgent need, not only for the regulator, but also the policy makers to ensure the existence and implementation of standards that would support interoperability of converging networks, and to ensure their coherence with international standards thereof.

A recommended solution here is for regulators of similar technologies, converging services and infrastructures, or standard controllers to collaborate their efforts, first, in defining interoperability and interconnection standards, and to collaborate enforcement methods. The SA Bureau of Standards can be a linking sector in this regard.

2.1.3 Matching international standards and practices

Today, national regulators are reshaping their activities according to new regional agreements, International Telecommunications Union (ITU), the General Agreements on Trade and Services (GATS) requirements. The case in point would be the new EU convergence regulations that seek to transform the way telecommunication and electronic technologies have been regulated in Europe (EU Green Paper, 1997), to be in line with regional economic integration. The OECD is another multi-

member institution that is updating its regulatory regimes along new convergence trends (James, 2001). Although to a limited extent, the same could be said of TRASA under the SADC region.

While the contents of such changes would be better discussed under a completely new topic, it is worth noting that national regulators will need to update themselves with changes beyond their borders if they are to be effective.

ICASA for example, would need to fulfil its national regulatory duties, and also comply with regional arrangements at the Telecommunications Regulators Association of Southern Africa's level in this respect (TRASA, 2001). An under-funded and institutionally incapacitated regulator may lack capacity to update itself with ever-changing technology standards, and to catch up with changes elsewhere (InfoSat news, 2002). This is a structural problem that requires a redefinition of relations between a regulator and political masters, as well as a rethink in the way regulators are funded.

2.1.4 Balancing e-commerce and cyber trade practices with convergence trends

Digital technologies and services offer effective, speedy and convenient ways of conducting business and trade. With modern technology, different products can now be advertised, bought and sold over the Internet, between strangers in different parts of the world. It is now possible to effect a banking transaction over the network, without even setting one's foot in the bank. Together with this development however, are borderless challenges that it raises. It raises *consumer protection issues*, and those of *copyrights* and *intellectual property rights*, different levels of *cyber crime*, and the new *contractual enforcement* issues that come with *cyber interactions*. Different nations however, have set in place e-commerce laws directed at regulating cyber trade, and to set in place mechanisms through which cyber crime could be controlled.

The shortfall with most of these policies, argues the EU commission, is that most of them are trapped in traditional methods of regulating diverged networks, infrastructures, and services (EU Green Paper, 1997). In this respect, the OECD and the EU among other international structures, are debating measures to update their policies not only to suit regional integration, but also convergence of new technologies (OECD, 1997). South Africa is also setting in place a number of laws, though under different departments, to address these issues (see section 2.3 below).

Together with policy reforms, international structures are adopting different measures to update compatibility of governing institutions, with new convergence trends and practices.

2.2 Updating compatibility of governing Institutions to Convergence Practices

Convergence highlights differences and similarities in regulatory requirements between converging sectors, and problems of overlap in the jurisdictions of separate regulators (OECD - DAFFE/CLP, 1999:7). Convergence between broadcasting, Internet, other sources of media, and telecommunications for example, may result in an overlap in services offered between sectors. At the same time, this may lead to conflicting interests between advertisers who could be competing for similar audiences across sectors where regulatory practices for competition are separate and uncoordinated (ibid). To address this challenge, regulators in many countries are merging overlapping sections and departments into single and coherent regulatory structures.

Trends towards the establishment of cross-sectional 'functional' regulators have emerged in many nations and institutions in the recent past:

⇒ The Federal Communications Commission (FCC) in the USA represents the oldest regulator to regulate across telecommunications, media, and broadcasting services (FCC, 2001).

⇒ In December 2001, the National Communications Authority (ANACOM) of Portugal began to integrate regulatory activities for Post, telecommunications, and broadcasting in December 2001, to accommodate convergence in technologies (ANACOM, 2001).

⇒ In April 2001, KommAustria and the Telekom Control Commission merged to form a *converged regulator, the* 'Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR GmbH) (RTR GmbH, 2001).
⇒ In March 2001, a broadcasting regulator, the Independent Media Commission (IMC) merged with the telecom regulator, the Telecommunication Regulatory Agency (TRA) to form the Communication Regulatory Agency (CRA) in Bosnia and Herzegovina. With this step Bosnia and Herzegovina joined other European countries, which are following world – wide trend of converging technology and transmission methods (CRA, 2001).
⇒ In 1996, the Botswana Telecommunications Authority (BTA) was formed and mandated to regulate broadcasting and telecommunication (BTA, 2001).
⇒ The Canadian Radio-Television and Telecommunications Commission is a converged regulator of broadcasting and telecommunications (CRTC, 2002).
⇒ In line with international trends, the Independent Broadcasting Authority (IBA) and the South African Telecommunications Regulatory Authority (SATRA) merged into the Independent Communications Authority of South Africa (ICASA) in July 2000. This was to facilitate effective and seamless regulation of telecommunications and broadcasting, and to accommodate the convergence of technologies (ICASA, 2000).

The advantage with this move is that it brings together regulators of services of similar networks under one authority, thereby enabling organisations in services offered by single networks to deal with a single authority. It further simplifies the regulation of these converging technologies and services. With the Internet becoming the nucleus of convergence then, perhaps ICASA and the Internet regulator should also consider closer cooperation in South Africa.

While this move may enable uniform and effective regulation across newly converging technology and service sectors, it would all be futile unless accompanied by mutually supportive policies and regulations across related sectors. Policy makers and regulators should update policies to suit new e-commerce and convergence trends for the regulatory framework to be relevant to changing times.

2.3 Improving traditional policy-making and implementation methods to suit convergence trends

As technology convergence becomes limitless, it will no longer suffice for nations to develop broadcasting or e-commerce policies distinct form IT trade strategies, or health and educational policies separate from communication and information policies. In this regard, many countries realise the significance of integrating various policy initiatives and implementation projects into single coherent strategies that will help them succeed and survive in the information era (Naude, 1999).

In addition to converging regulator institutions, different governments are beginning to amend traditional laws and regulations upon which regulators' mandates are derived, to suit integrating regulatory frameworks:

⇒ The EU began a Green Paper process in 1997, and an ongoing debate on improving traditional regulatory and policy methods of different regulators in its integrating member states, to be coherent and inline with new technological innovations, and more enabling to convergence (EU Green Paper, 1997).
⇒ The convergence of the broadcasting and telecommunications regulators into the CRTC in Canada was followed by amendments - to enable coherence in laws upon which a converged CRTC derives its mandate. The converging laws are: - the *Broadcasting Act* (S.C. 1991, c. 11, as amended), the *Telecommunications Act* (S.C. 1993, c. 38, as amended) and the *Bell Canada Act* (S.C. 1987, c.19 as amended) (CRTC, 2002).
⇒ The convergence of the IBA and SATRA into ICASA was accompanied by the indirect convergence of four policies that define ICASA's mandate: the statutes include the ICASA Act of 2000, The Independent Broadcasting Act of 1993, the Broadcasting Act of 1999, the

Telecommunications Authority Act No. 103 of 1996, and the Telecommunications Amendment Bill no 64 of 2001. Other than these laws, convergence at policy level in SA remains very minimal.

Convergence, as has been dominant in the EU and the OECD policy agendas since the mid-1990's is still an issue of policy debate in few developed countries. Whilst convergence at regulator levels is advanced in SA, convergence is more than just a regular issue. It extends to all policies that relate to e-commerce, manufacturing, security, and cyber trade as regulated by different government departments. Such laws include: the Interception and monitoring Bill of the Department Justice, the general Competition Act of the Department of Trade and Industry, the HANIS Bill as proposed by the Department of Home Affairs, and the Electronic Communications and Transactions (ECT) Bill of the Department of Communications. These sets of legislations regulate certain sectors of converging technologies, yet are implemented and enforced by different institutions, with very little national debate on how they would enable convergence.

In other words, convergence of five laws upon which ICASA derives its mandate in SA may not adequately enable effective regulation under convergence without coherence of cross-sector policies. This could be made possible, first, by a deliberate process of national policy debate on the coordination of convergence related policies and regulations. Secondly, by the integration of related contents among different policies directly related to convergence regulation. The following section, section 3, discusses different items of a single set of legislation, the ECT Bill, and analyses how this legislation would impact the future of cyber-trade, and the implications it would have on the regulatory regime, the industry and society.

3 SA Policy and Convergence

Technological innovations are taking place faster than regulatory developments. The danger this poses is a possible inability of the regulatory regime to catch up with convergence changes. This could be followed by ineffective regulation due to increasing incompatibility of traditional regulations and practices on converging technologies and services. Leading to a limited control on ever advancing cyber-crime, failure to protect consumer interests, and a declining order in the cyber-market and trade.

This could be averted only if regulatory regimes could leapfrog development gaps between technology innovations, and regulatory frameworks, policies and applications. In this regard, deliberate national strategies that will neutralise challenges of regulating new technologies are becoming imperative for policy and regulatory regimes around the world. While regulators of traditionally separate, but related sectors are converging in many parts of the world – including SA, there is a growing need for new policies and regulations to be drafted so as to enable regulation of converging sectors and services. While regulatory gaps are evident in the new Telecommunications Amendment Act (2001), the question remains as to how the new ECT would enable effective regulation of the newly converging technologies. The following passage attempts to find answers to this question.

The ECT Bill (2002) and Convergence

The following items of the ECT Bill will have mixed impacts on the regulation of converging technologies:

(1) Regulating the formulation of the Electronic Transactions Policy
(2) Setting up of legal requirements for data messages
(3) Provision for the authentication of electronic services
(4) Provision for the protection of consumer interests
(5) Provision for the protection of personal information
(6) Provision for the introduction of cyber inspectors
(7) Provision for the control of cyber crime, and
(8) Provision for the setting up of the national e-strategy

3.1 Regulating the formulation of the Electronic Transactions Policy

Chapter II (Sec10) of the Bill recognises the need for the electronic transactions policy in SA, and makes a provision for the minister of communications to formulate such a policy.

While this provision requires the minister to consult the cabinet and other ministers of relevant departments, and to publish the policy guidelines, no mention is made in this regulation, that the future policy should address convergence issues.

Critique and Recommendations:

Recognising the need for this development represents a positive step towards the preparation of the regulatory framework to match modern technological developments. However, making policies for their own sake, without emphasising to update their contents to meet new technology challenges could be inadequate.

Policy makers should use this opportunity to introduce the national debate on how *convergence-readiness* of future electronic transactions policies could be ensured. With the policy formulation debate addressing the question of effective implementation of such a policy, across technologies and sectors. The consultative process should extend beyond cabinet circles, to wider sectors as possible in this issue.

3.2 Setting up of legal requirements for data messages

With convergence in technology capabilities, it is now easier for user of a telecommunications infrastructure or technology to transmit data or audio message, via any other network, to any other telecommunications technology anywhere in the world. Along with this development, contractual and legal regulations are also expanding. Network users should be able to conduct enforceable business transactions using data messages. For a data transaction to be legally enforceable, however, legal recognition of data messages should be established.

Chapter III (Sec 11) of the ECT Bill sets out the legal requirements of electronic data messages, thus enabling the regulation and legal enforcement of electronic transactions over any network or service:

The regulation attaches a legal status to any electronic message that can be sent, received, read, printed, accessed in anyway, and stored (Sec.3 (b); and Sec. 12 (a), (b); and affords a legal status to electronic signatures (Sec 13.1). Section 13 (2) further provides for assessments of electronic signatures, and to ensure that fraudulent alterations in electronically signed data are detected. Data messages are fully acceptable as original documents (Sec.14), and as valid evidence in the courts of law (Sec. 15.1,2,3). Sections 23, 24, 25, 26 and 27 provide the framework that incorporates electronic transactions into the general mercantile law practices.

Critique and Recommendations:

This provision applies to all electronic transactions across networks and infrastructures. More positive is that it also puts electronic transactions in par with the general laws of other commercial transactions. Such legal clarity on electronic data and signatures would enable the regulation of electronic transactions across converging technologies, and the integration of electronic transactions with commercial transactions. And as such, is commendable.

All being said however, section 20 of this regulation subordinates this provision to other laws that may regulate to the contrary. Failure of this stipulation or the whole legislation to override contrary regulations in any other separate law could complicate its implementation where a transaction is regulated by another contrasting law. A recommendation would be for the future electronic transactions policy to cover this vacuum by making regulations that would override all other laws if the manipulation of the regulatory system were to be avoided.

3.3 Provision for the authentication of electronic services

Recognising electronic data and signatures can only serve the desired ends if the authenticity of such services can be protected, checked and verified.

In this respect, chapter VI of the ECT Bill provides for the assessment of the authenticity of electronic data, transactions, and signatures; the formation of authentication and accreditation authorities:

Section 35 empowers the Director General of Department of Communications and the department staff the status of an authentication authority. The authority appoints *authentication service providers*, accredits authentication equipments used, and appoints independent auditors to ensure compliance with regulations. Section 39 outlines the criteria for the accreditation of authentication equipment, and accreditation revocation measures in section 40.

Critique and recommendations:

It is useful for the regulatory regime to have the authentication mechanism in place. However, too much power and discretion is given to the minister, and the department officials. It does not leave enough room for an independent authority in case of a dispute being between the government and the private party. Instead of providing for the Director General and the departmental staff the Authority status, it could be more neutral and therefore appropriate to provide for an independent commissioner to perform the task. The minister however, could be sufficient where the government remains a non-party to possible consumer and public protection issues, something that cannot be guaranteed, and therefore should not be left to chance.

3.4 Provision for the protection of consumer interests

One of the functions of regulators is to set equipment standards and enforce regulations for the protection of the customer and public interests (ICASA, 2002). The regulatory regime however, needs a relevant and an enabling legislation to effectively fulfil this task.

The relevant regulation in this regard is chapter VII, which provides for the protection of customer interests in electronic transactions and services:

To protect the consumer, Sec 44(1) requires a supplier in cyber trade to make full disclosure of its full name; physical address and phone number; legal status; code of conduct; sufficient characteristics of electronic goods or services offered; the prices; the time for, and manner of, dispatch; the refund policy; the security procedures; and privacy policy in respect of payment. The supplier should further allow the consumer the opportunity to view the electronic transactions and to correct any mistakes, or the chance to withdraw from the transaction before finally placing an order. The customer is also allowed to cancel the transaction within seven of receipt of goods or services (Sec. 45), with refund entitlement. This stipulation extends to all electronic transactions, irrespective of the legal system applicable to a particular agreement (Sec 48). The consumer may further complain to the consumer affairs committee, in case of non-compliance by the supplier (Sec.50).

Critique and recommendations:

This provision covers a large scope of converged technologies. Although no attempt or mention was made to regulate for converging technologies and transactions, the scope it covers would enable effective regulation and protection of consumer interests in electronic transactions and convergent services. Cyber-trade however, has no boundaries. There is a need for clarity on how local consumers would be protected against unfair practices by foreign suppliers, without locals incurring high international legal costs. Perhaps the future electronic transactions policy could address this area more clearly.

3.5 Provision for the protection of personal information

With cyber-trade, personal and sometimes confidential information is increasingly exchanging destinations via multiple networks. Even when a stranger end-user of confidential information could be relied upon, criminals can easily intercept personal information when it is negligently handled or inadequately protected.

To regulate against this challenge, chapter VIII provides for the protection of personal information in electronic transactions:

Section 52 (1) provides for a complete confidential handling of customer personal information by data controllers, except when they are required by law to disclose information, in which case, the customer is to be informed in writing.

Critique and recommendations:

The provision is useful as a guide, but fails consumers by allowing a party controlling personal information the discretion to freely trade with such information (Sec.52 (9)), and makes no safeguards against possible use to the detriment of the customer. An example here would be such a free use of information to gain a competitive advantage against the customer in case the customer enters in a similar trade with the data holder. This shortfall should be averted in the future electronic transactions policy.

3.6 Provision for the introduction of cyber inspectors

The existence of enabling regulations and compatible structures should be complimented by effective enforcement measures.

To meet this purpose, chapter XII of the ECT Bill provides for the appointment of cyber inspectors to inspect compliance of the industry with laid down regulations:

Section 84 authorises the Director General to appoint such inspectors and afford them with a certificate of appointment to be shown when performing inspection duties. Section 85 outlines the powers of the inspectors as extending across the monitoring and inspection of web sites, cryptography services, and authentication services, their premises or their information systems. Inspectors can assist and be assisted by statutory bodies such as the South African Police Service (Sec.85 (2)). Section 87 requires inspectors to obtain searching warrants from any court to conduct specific inspections. Section 88(1) outlines the inspector's obligation of non-disclosure of information obtained during inspection, except for purposes of law enforcement.

Critique and recommendations:

This provision would enable effective investigations, and eventually effective regulation and enforcement of regulations. However, while cyber-trade and cyber-crime tend to defy national borders, this provision is failing to account for interference with local regulations by international bodies. Relations with foreign regulators and law enforcement agencies should be promoted if effective regulation of the borderless cyber trade is to be enhanced.

3.7 Provision for the control of cyber crime

The fast pace in which technology innovation unfolds is strongly challenged by similar developments in cyber crime. There is a need for regulatory regimes to develop strong and effective crime control measures across converging technologies, and beyond their national borders if the benefits of innovations are to be maximised.

Chapter XIII of the ECT Bill provides for the control of cyber-crime:

Section 90 re-iterates the provisions of a separate law, the "*Interception and Monitoring Prohibition Act (Act no.127 of 1992)*"that it is an offence for any unauthorised persons to monitor and intercept any data in any network or information systems. Outlined in sections 90 to 93 are what is considered as unlawful acts, including hacking of electronic and computer networks. Section 94 integrates the punitive measures of enforcement procedures with the general criminal procedures as provided in the criminal procedure Act (no 51 of 1977).

Critique and recommendations:

This provision describes cyber-crime as referring to unauthorised interception and monitoring, as well as hacking. While these are major elements of cyber-crime, criminal activities are so broad and too diverse to be reduced into these few activities. While it is useful to outline these activities as unlawful, perhaps the provision should have been more general and broad, as well as accommodative of more convergence between electronic services' regulations and other law enforcements. This being said, it is recognised that offences of all sections of this legislation are equally criminal, and by default, are elements of the cyber-crime control system.

3.8 Provision for the setting up of the national e-strategy

As convergence between networks and services increases, all affected sectors affected will require a clear and predictable regulatory framework to facilitate investment decisions. As services overlap, coherence between traditional policies – into a common regulatory regime in electronic transactions and converged technologies is becoming imminent.

Attempts to address this challenge are made in the ECT Bill, by the provision in chapter II, for the formulation of a broader National e-strategy:

The strategy, which should become national priority, will determine all matters involving e-government, electronic communications and transactions (sec 5(4)). The strategy will distinguish between national, regional, continental, and international strategies. It will also outline programmes to achieve universal access, human resource development and Small, Micro, and Medium Enterprises (SMMEs) development and the overall e-readiness of SA.

Critique and recommendations:

Although the provision is silent about convergence, one may deduce from its broadness that it also covers issues of this development. One can only recommend a thorough consultative process rather than to just limit the debate to the cabinet ministers as is stipulated in the provision. Lessons from the EU green paper and a consultative process of market, industry, and society stakeholders is strongly recommended in the policy formulation process.

4. Conclusion

Technology convergence offers massive opportunities for the development of new services and the expansion of consumer choice. It enables a substantially higher capacity of *traditionally distinct voice* and *data* transmission services to be transported over similar networks and to use integrated consumer devices for purposes such as telephony, television or personal computing (PC).

Together with these advantages also emerge new and systematic changes to traditional ways of regulating the manufacturing and trade in converged IT, media and telecommunications goods and services within and between countries. These changes are imposing new challenges on the regulatory regime, industry, markets, and the society at large. Different nations and institutions are applying various measures and changes in their policies, regulations, and institutional frameworks to meet new convergence related challenges. OECD countries and the EU are updating regulatory frameworks to match new industry, market, and public protection issues brought about by converging technologies.

Attempts are also made to integrate national regulatory practices to match international agreements, and to updating compatibility of governing institutions to convergence practices.

Convergence, as has been dominant in the EU and the OECD policy agendas since the mid-1990's is still an issue of policy debate in few developed countries. Whilst convergence at regulator levels is advanced in SA, convergence is more than just a regular issue. It extends to all policies that relate to e-commerce, manufacturing, security, and cyber trade as regulated by different government departments. Such laws include: the Interception and monitoring Bill of the Department Justice, the general Competition Act of the Department of Trade and Industry, the HANIS Bill as proposed by the Department of Home Affairs, and the Electronic Transactions Bill of the Department of Communications. These sets of legislation regulate certain sectors of converging technologies, yet are implemented and enforced by different institutions, with very little national debate on how they would enable convergence.

In other words, convergence of few laws upon which a regulator derives its mandate in SA may not adequately enable effective regulation under convergence without coherence in cross-sector policies. This could be made possible, first, by a deliberate process of national policy debate on the coordination of convergence related policies and regulations. Secondly, by the integration of related contents among different policies directly related to convergence regulation.

Several attempts are made in the ECT Bill, to improve the regulation of cyber-trade, of interactions in electronic transactions, the industry, control of cyber crime, and the protection of consumer interest, as well as the provision for the formulation of a coherent national e-strategy.

There are evident shortfalls in the manner in which the ECT Bill attempts to address convergence issues:

- ⇒ The provision for the formulation of the national electronic transactions policy is important. But limiting the consultation process only to cabinet and other ministers of relevant departments would limit the scope of the policy. While the minister will be required to publish policy guidelines afterwards, omission of a broader industry consultation process as is the case in the EU, and that the future policy should address convergence issues may limit the debate, and eventually the contents of the new policy.
- ⇒ While chapter III sets out legal requirements for electronic transaction, section 20 unfortunately subordinates such a provision to any other contrary regulations.
- ⇒ Updating policies to match convergence practices is not emphasised in the ECT Bill
- ⇒ Clarity is lacking on the consultative scope of the national debate that will shape the national e-strategy. Learning from the EU consultative process that followed the 1997 Convergence Green Paper is recommended in this respect.

5. References

Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR GmbH) http://www.rtr.at/web.nsf/englisch/startseite?Opendocument

Bosnia and Herzegovina - The Communication Regulatory Agency (CRA) http://www.imcbih.org/

Botswana Telecommunications Authority (BTA), http://www.bta.org.bw/about.html

Cape Times – Business Report: Matsepe – Casaburri intent on resolving telecoms tariff issue, 27 May 2002: p1

Electronic Communications and Transactions (ECT) Bill

European Commission (EC), Green Paper - the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation. Towards an Information Society Approach', European Union (EU), Brussels, 3 December 1997, http://europa.eu.int/ISPO/convergencegp/greenp.html

EC, Working Document - The Commission summary of the results of the public consultation on the green paper on 'Convergence Of The Telecommunications, Media And Information Technology Sectors'; EU, Brussels, 29 July 1998, http://europa.eu.int/ISPO/convergencegp/workdoc/1284en.html#1.%20http://www.ispo.cec.be

European IT Conference & Exhibition (EITC' 97) "Convergence: Creating the Future" Brussels Congress Centre, 24-26 November 1997, http://www.cordis.lu/esprit/src/eitc97an.htm

Federal Communications Commission, USA (FCC) http://www.fcc.gov/aboutus.html

Independent Communication Authority of South Africa, (ICASA) http://www.icasa.org.za/?FromHome=1&Cmd=ViewContent&ContentID=180

InfoSat News, 'ICASA needs muscle as competition intensifies', 10 April 2002, http://www.infosat.co.za/news_get.asp?NewsID=220&Opt=&Data=&RecNum=1

Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992)

James, Charles, A. 'International Antitrust in the 21st Century: Cooperation and Convergence'. Discussion Paper on the OECD Global Forum on Competition, Paris, October 1997.

Kenwood, C.A. 'A Business Case Study of Open Source Software'; The MITRE Corporation, July 2001, Washington C3 Center, Bedford, Massachusetts http://www.mitre.org/support/papers/tech_papers_01/kenwood_software/

Langa, Mandla, Independent Communications Authority of South Africa (ICASA), Cape Times - Business Report, 8 May 2002: p2

Link Centre, Convergence and Broadband Implications for South Africa. Submission to the Department of Communication Stakeholder Colloquium on New Telecommunications Policy for South Africa, 22 January, 2001 http://docweb.pwv.gov.za/docs/telesubs/centre.PDF

Makhaya, G. - The determinants of regulatory effectiveness in liberalised markets: developing country experiences'. Wits University, 2001

National Communications Authority of Portugal, http://www.icp.pt/index.jsp?categoryId=2958

National Communications Authority of Portugal, http://www.icp.pt/template20.jsp?categoryId=4675&contentId=17645

Naude, Pieter; *Dimension Data*, 'New Telecommunications Policy For South Africa', 1999

Organisation for Economic Co-operation and Development (OECD), DAFFE/CLP (1999)1

Organisation for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Policy: Global Information Infrastructure –Global Information Society (GII-GIS). OCDE/GD (1997)139, Paris.

Sentech Multimedia services, Products: 'Data casting And Internetworking Via Satellite' 2002. http://www.sentech.co.za/satelite/products.htm

Squire, Sanders & Dempsey L.L.P. and Analysys Ltd, prepared for the EC - 'Study For EC DG Information Society: Consumer Demand for Telecommunications Services and the Implications of the Convergence of Fixed and Mobile Networks for the Regulatory Framework for a Liberalised EUMarket', Brussels-Luxembourg, January 2000. http://europa.eu.int/information_society/topics/telecoms/radiospec/doc/pdf/mobiles/study%2000.pdf

The Criminal Procedure Act, 1977 (Act No. 51 of 1977),

Washington Post, 'Digital TV's Big Hurdle: Copy Protection', Wednesday, 5 June 2002 http://www.washingtonpost.com/ac2/wp-dyn/A60770-2002Jun4?language=printer

Also see - http://www.sn.apc.org/nitf/converge/sld029.htm