# South Africa Cyberlaw and ICT Conference


## Proceedings of Lex Informatica 2009

Johannesburg
South Africa
July 22-24

# Lex Informatica 2009: South Africa Cyberlaw and ICT Conference

## Johannesburg, South Africa
## July 22-24, 2009

**Conference Organizer and Chair**

Sizwe Lindelo Snail, LLB
Couzyn Hertzog & Horak
Pretoria, South Africa




**ADFSL**

**Association of Digital Forensics, Security and Law**



ISSN 1949-1344

# Sponsors

## Conference Committee

Lex Informatica 2009: South Africa Cyberlaw and ICT Conference is pleased to have the following as members of its conference committee.

# Contents

# Preface

The papers published in these conference proceedings are from the 2009 Lex Informatica conference, *Convention on Lex Informatica – Practical Application of Cyberlaw in Different Environments (2009)*. The conference was organised by the law firm of *Couzyn Hertzog and Horak* and held from the 22nd to the 24th of July 2009 at the Birchwood Conference Centre in, Johannesburg, South Africa. The 2009 Lex Informatica conference was dedicated to Information Technology Law in South Africa. The contributions published in this issue address the Legal Effect of South African E-commerce, the Electronic Communication Transactions Act of 2002, E-consumer Protection, Domain Name Dispute Resolution and Sexual Exploitation on the Internet. Three of the papers presented at the conference were also chosen as best papers and published as peer-reviewed articles in volume 4 number 4 of the Journal of Digital Forensics, Security and Law (JDFSL).

**Francis Cronjé**'s article gives a broad overview of some of the problems South Africa is experiencing within its current status on privacy. The author concludes that the solution for these problems does not necessarily arrive with the issuing of the codes of conduct themselves, but rather through a preemptive strike and pro-active based effort on behalf of the specific sectors to submit such codes to the Privacy Commissioner for approval.

**Jacqueline Fick** in the article *Prevention is better than Prosecution* proposes that effectively and efficiently addressing cyber crime requires a shift in paradigm. She points out that businesses and government departments alike the focus should be on prevention, rather than the prosecution of cyber criminals. She concludes that the shift in this paradigm from a re-active to a pro-active approach and focusing on prevention rather than the prosecution of criminals that attack computer systems, poses benefits in terms of cost, time, resources and organisational reputation.

We are also pleased to include the conference paper by **Z. Ntozintle Jobodwana** on telecommunications liberalization in Africa. In this paper, the author demonstrates how telecommunications and information technology present copious opportunities for the creation of unprecedented wealth for Africa. He concludes that African countries may benefit from these opportunities by removing policies that fostered and encouraged the dominance of the public sector in national economies in order to attract modern industries and business.

*Is South Africa's ICT Regulatory Framework Still a Barrier to Entry?* by **Carmen Cupido** discusses how South Africa's ICT regulatory framework is the factor that keeps prices for communication high. The author outlines certain salient aspects of the regulatory framework in South Africa, including the e-rate, expanded consumer protection and universal service obligations, within which new entrants operate in the electronic communications services sector.

The article by **Omphemetse Sibanda** discusses how the promotion of access to Information Act of 2000 in South Africa places an obligation on e-government services to be more accessible, including taking appropriate steps to bridge the digital divide particularly in cases where the services are offered primarily or substantially through ICT facilities. To overcome challenges related to ICTs, which may impact on individual Departments' e-governance processes, the author feels DIA should introduce or develop ITC software in other local languages to make its website more accessible since the lack of African languages software is a barrier that prevents full access and enjoyment of services and of exposure to DIA's e-services.

The paper by **'Dejo Olowu** recognises the phenomena of cybersquatting and typosquatting as a problem that exists because of the Internet, and which is likely to continue into the future. The paper contributes a voice to the philosophical thinking that inevitably underpins the innovative attitude of law courts and other quasi-judicial bodies dealing with domain name disputes. An attempt has been made by the author to accentuate the location of domain name disputes and the incidence of cybersquatting within the realm of property law.

I am also pleased to include the conference paper by **Adedamola Owolade** and **Sizwe Snail** on sexual exploitation of children and adolescents via cyberspace. The authors identify the incidence of online sexual exploitation in South Africa and compare the extent of this threat with countries with similar income and social profile. They conduct a comparative legal survey on how lack of regulation and lack of law enforcement perpetuates the sustained occurrence of these immoral and illegal practices. To develop transnational policing capability, the authors feel a global co-operation between source and destination countries is absolutely imperative.

Lastly, we are also pleased to include the conference paper by **Milton Luoma** and **Vicki Luoma** on ethical hacking. The authors analyse the debate on whether a legal distinction between white hat hackers and black hat ones should exist or not? They present a case study on students who hacked the security features of Boston Subway system to show its vulnerabilities. They conclude that there is no provision for either a white hat or research exception to the law.

I would like to thank Dr. Glenn Dardick, Editor-in-Chief of the JDFSL for graciously putting these proceedings together as well as creating the special issue of the JDFSL. I would also especially like to thank Sizwe Snail and the law firm of Couzyn Hertzog and Horak for making this conference possible.

Judge Mohamed CHAWKI, Ph.D
Chairman, International Association of Cybercrime Prevention
Paris, France

## Acknowledgments

I would like to thank “my team” of candidate attorneys Ms Marelize Gloy, Ms Precious Mnisi, Mr. Bruce Rokho (who has since been admitted as an attorney-“Congratulations”) and Mr. Joel Mohlamonyane (who has also since been admitted as an attorney -“Congratulations”) for the assistance and dedication to this project. Without you guys it would have not been possible.

Thank You.

Sizwe Snail
Chair, Lex Informatica 2009
Couzyn Hertzog & Horak
Pretoria, South Africa

# Schedule

**First Day of Proceedings: 22 July 2008**

**08:30–08:45** Mr Joel Mohlamonyane, Attorney, Couzyn Hertzog & Horak Inc.
Welcome Address

**08:45-09:00** Mr Sizwe Snail, Conference Chair, Couzyn Hertzog & Horak Inc.
Introduction of Keynote Speaker for the day

**09:00–09:55** Dr Glenn Dardick, Assistant Professor of Information Systems, Longwood University, USA and Adjunct Associate Professor, School of Computer and Information Science, Edith Cowan University, Australia
Keynote Address: Digital Forensics Assurance: Assuring Non-Repudiation

**SESSION I: E-Commerce Session**
CHAIR OF SESSION: Prof Tana Pistorius, UNISA

**PANELISTS**: Prof Tana Pistorius, UNISA
Dr Glenn Dardick, Longwood University, USA

**10:30-11:20** Prof Tana Pistorius, UNISA
WEBSITE COMPLIANCE IN TERMS OF ECTA

**11:25-12:15** Mr Sizwe Snail, Couzyn Hertzog & Horak Inc
ELECTOCNIC SIGNATURES: COMPARATIVE PERSPECTIVES ON SA, US & EU LAW

**12:20-13:10** Mr Francis Cronje, PRICE WATERHOUSE COOPERS
An overview of Data Protection

**13:15-13:30** PANEL DISCUSSION

**SESSION II: Cyber Crime and Forensics**
CHAIR OF SESSION: Dr Glenn Dardick, Longwood University, USA

**PANELISTS**: MrJoel Mohlammonyane, Attorney, Couzyn Hertzog & Horak Inc.-
Dr Annamart Nieman, Deloitte and Touche
Reinhardt Buys, Deloitte and Touche

**14:30-15:20** Akalemwa Ngenda, Brunel Law School - UK
The Emerging Cyberlaw Regime in Zambia

**15:20-16:15** Mr Reinhardt Buys, Deloitte and Touche
LOSING GROUND - KEY FINDINGS OF THE 2009 GLOBAL DATA SECURITY SURVEY

**16:20-17:00** Adv. Jacky Fick, PRICE WATERHOUSE COOPERS – South Africa
Prevention is better than Prosecution: Deepening the defence against cyber crime

**17:00** Dr Glenn Dardick, Longwood University, USA
Close of day's proceedings

# Schedule

**Second Day of Proceedings: 23 July 2009**

**08:30-08:45** Mr Bruce Rokho, Couzyn Hertzog & Horak Inc
Welcome Address and Introduction of Keynote Speaker for the day

**08:45-09:15** Dr Vicki Luoma, Minnesota State University, USA
Keynote Address: "E-Jurisdiction problems"

**SESSION III: Intellectual Property, Online Delict & Crimes**
CHAIR OF SESSION: Prof Tana Pistorius, UNISA

**PANELISTS**: Mr Sizwe Snail, Couzyn Hertzog & Horak Inc.
Mr Daniel Greenberg, Lexinergy - UK
Ms. Pria Chetty, Chetty Law

**09:15-10:00** Mr Daniel Greenberg, Lexinergy - UK
COM VS TM, WHO WILL WIN?

**10:30-11:20** Mr. Lobo Das Neves, International Law Enforcement Institute
Electronic communications and the Drug Trafficking

**11:25-12:15** Ms. Pria Chetty, Chetty Law
Managing Legal Risks attached to Social Media

**12:20-13:10** Prof. Dejo Olowu, Walter Sisulu University
Domain names

**SESSION IV: Civil Procedure In E-Commerce , Privacy & E-Governance**
CHAIR OF SESSION: Adv Ntozintle Jobodwana, UNISA

**PANELISTS**: Mr Brendon Hughes, Michalson Attorneys / Infology
Adv Ntozintle Jobodwana, UNISA

**14:30-15:10** Mr Brendon Hughes, Michalson Attorneys
Analysis of the Rules of Court in light of the Electronic Communications and Transactions Act No. 25 of 2002.

**17:00** Dr Vicki Luoma- Minnesota State University, USA
Close of proceedings DAY 2

# Schedule

**Third Day of Proceedings: 24 May 2008**

**08:45-08:55** Mr Sizwe Snail, Couzyn Hertzog & Horak Inc
Opening Address and Introduction of Keynote Speaker for the day

**08:55-09:45** Adv. Jobodwana, UNISA
Keynote Address: TELECOMMUNICATIONS LIBERALISATION IN AFRICA: PROPOSED REGULATORY MODEL FOR THE SADC REGION.

**SESSION V: ICT & TELECOMMS**
CHAIR OF SESSION: Ms Carmen Cupido, Bowman Gilfillian

**PANELISTS**: Mr Sizwe Snail, Couzyn Hertzog & Horak Inc
Ms. Kerron Edmunson, Kerron Edmunson
Ms Carmen Cupido, Bowman Gilfillian

**9:45-10:45** Ms. Kerron Edmunson, Kerron Edmunson
TELECOMS REGULATION IN SOUTH AFRICA

**11:00-12:00** Ms Carmen Cupido, Bowman Gilfillian
Impact of RICA Amendments and Directives on the Electronic Communications Industry.

**SESSION VI: VARIOUS LEGAL MATTERS**
CHAIR OF SESSION: Mr Barend Burgers, Barend Burgers Attorneys

**12:00-13:00** Prof Omphemetse Sibanos, UNISA
Shedding the Horror Affairs Image: Towards True and Sustainable Departmental e-Interconnectivity and e-Delivery for the South African Department of Internal Affairs

**14:00-15:00** Mr Sizwe Snail, Couzyn Hertzog & Horak Inc
Mr Damola Owolade, University of Pretoria
Sexual Exploitation in the online world – A South African perspective

**15:00** Mr Barend Burgers, Barend Burgers Attoneys
BEST CREATIVE AND BEST RESEARCHED PAPER AWARD

**15:15** Mr Sizwe Snail, Couzyn Hertzog & Horak Inc
Close of conference

# A Synopsis of Proposed Data Protection Legislation in SA

**Francis S Cronjé**
KPMG Services (Proprietary) Limited
Parktown, South Africa
francis@cybersmart.co.za

Privacy International[1] made the following statement regarding South Africa's financial sector in its 2005 world survey:

> "South Africa has a well-developed financial system and banking infrastructure. Despite the sophistication of the financial sector, the privacy of financial information is weakly regulated by a code of conduct for banks issued by the Banking Council."

This extract highlights some of the problems South Africa are experiencing with its current status on privacy as viewed from an International perspective. In recent years the International society has stepped up its efforts in creating a global village wherein the individual could be assured of having his/her privacy protected. Various conventions and guidelines[2] have previously laid the foundation for privacy but it was not until the European Union's (EU) launch of its Directive on Data Protection in 1995 that we have seen a real coerced shift in the focus of such protection. Cross border data transfers from the EU became something of the past unless third countries (those countries outside the EU) could prove the existence of adequate data protection provisions. It seemed to a big extend that international trade would be hampered and some of its biggest trading partners, such as the US, suddenly felt the impact due to its lagging protection measures. In order to curtail such inadequacies, a Safe Harbor Agreement was entered into between the EU and US whereby cross border data flow would be allowed under certain prerequisites. This Agreement however, does not cover Financial Institutions.

Concomitantly, South Africa, having the EU as its biggest trading partner also felt the grunt and some SA organizations had to take its processing to within the borders of the EU.[3] By implication it was then assumed that South Africa lacked the adequacy criteria as laid down by the EU Directive on Data Protection.[4] The South African Law Reform Commission (hereinafter referred to as SALRC) instructed a project committee to work on a draft Bill on Protection of Personal Information (hereinafter referred to as POPIA).

Some of the reasons why, can best be explained as Prof Iain Currie reflects in his summary of the proposed POPIA:

---

[1] Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, medical privacy, and freedom of information and expression. Available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65428 (17 August 2007).

[2] a) The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention); and

b) the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.

[3] Nedbank (one of the big five banks in South Africa) has accordingly been forced, in the absence of such legislation locally which would have facilitated the bank processing information within South Africa, at great extra cost, to set up processing centres in Europe, in order to meet European information protection legislative requirements. This has resulted in the effective cost to market of the bank's outsourcing service being driven up and could very well be the reason for preventing the bank from obtaining further business processing outsourcing deals within Europe on the basis of not being cost competitive enough. (Comments on SALRC draft proposal)

[4] Art 25(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. Also refer to Art 29 Working Party's Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data. (Annex to the Annual Report 1998 (XV D/5047/98) of the working party established by Article 29 of Directive 95/46/EC.)

> "South Africa has general privacy protection in the Bill of Rights [s 14]. The right is protected by a private law action to interdict current or anticipated privacy infringements or to recover damages for infringements that have already occurred. Though information privacy is encompassed in the constitutional protection of privacy, there is no specific legislative regulatory regime for this aspect of privacy. The Promotion of Access to Information Act [5]protects personal information from disclosure in response to a request made in terms of the Act, but has no application outside the context of such a request. It is this absence of legislation that the SALRC draft Bill intends to remedy."

Although there is current legislation in place, none are specifically formulated to address data protection. For instance, The Electronic and Communication Transaction (ECT) Act of 2002[6] also addresses the collection of personal information in its chapter 8 but subscription to such principles is voluntary. The Regulation of Interception of Communications (RIC) Act prohibits the interception of communications while one Act that has recently been enacted, The National Credit Act, makes specific provision for the regulation of personal information, although such regulation is restricted to the financial sector.

Should the POPIA be enacted, consequential amendments may be necessary in respect of the following acts: Banking Act 38 of 1942, Broadcasting Act 4 of 1999, Copyright Act 98 of 1978, Electoral Act 73 of 1998, Financial Advisory and Intermediary Services Act (FAIS) 37 of 2002, Financial Intelligence Centre Act (FICA) 38 of 2001, Regulation of Interception of Communications and Provision of Communications Related Information Act 70 of 2002, Short-term Insurance Act 53 of 1998, Long-term Insurance Act 52 of 1998 and Telecommunications Act 103 of 1996.[7] Subsequently, the Electronic Communications Act of 2005 might also be subject to amendments.

A survey of access to information laws and practices in 14 countries was done by the Open Society Initiative and published in its Justice in Action Series, tilted, Transparency and Silence. They had the following to say about South Africa:

> "South Africa, the only monitored country in Africa with a freedom of information law in place, demonstrated greater compliance with the right to information than the other four African countries. However, only 19 percent of the requests submitted in South Africa yielded a compliant outcome and only 13 percent yielded information. This is by far the lowest score of the seven monitored countries with freedom of information laws. Justice Initiative monitoring exercises in both 2003 and 2004 highlighted serious problems with the implementation of South Africa's Promotion to Access of Information Act (Act No. 2 of 2 February 2000), and these problems resulted in high levels of mute refusals in response to requests. Although the law is strong on paper, it has proved complex to implement in practise, and there have not been sufficient efforts to make its implementation a priority. Better implementation might yet make it a model for the region."

Clearly this is the last sort of comment that South Africa needs on the implementation of its proposed POPIA. Currently, as the draft stands, it is however not unforeseeable that such comment might well be read into its implementation, since some of its provisions might also prove too complex to implement in practise, especially seen from the banking industry's perspective.

Some of the issues are for instance the cross border data transfer problems related to payment orders. Other problems are those concerning fraud, Basel II and the legally non-binding codes of conduct that is currently laying the guidelines for banking practices with regards to its consumers.

The question would be whether there is a golden one rule solution. I sincerely doubt this. It is my contention

[5] Act No. 54 of 2002. View www.info.gov.za/gazette/**act**s/2002/a54-02.pdf (12 August 2007)

[6] Art 50(2) ECT Act.

[7] SALRC Discussion papers available at http://www.doj.gov.za/salrc/dpapers.htm (07 August 2007)

that an array of various factors must play a role in seeing the proposed POPIA through to its successful implementation. Such factors would include safe harbour agreements, technological solutions, and sector specific regulations in the form of privacy code of conducts.

For South African banks for instance to operate successfully in Africa, specifically in the SADC region (SADC stands for 'Southern African Development and Economic Community' and refers to 14 African nations[8] in Southern Africa, who have signed a mutual trade and co-operation agreement) it is my suggestion that South Africa sign a safe harbour agreement[9] with the other members of SADEC, similar to that as between the USA and the EU, but with the exception that it also makes provision for financial institutions,. None of theses countries[10] currently make provision for data protection in its laws. Without such an agreement, banks for instance might be strained along in subjecting themselves to unnecessarily high costs in it's strive to comply with the proposed POPIA. In signing such an agreement however, time limits must be set on these countries to implement similar legislation, encouraging them to step up its own democratic values in ensuring sufficient privacy measures and achieving the objectives and vision as set by SADC.[11] This would then set a standard for the rest of Africa and hopefully spirit them on to reach similar goals.

It is also suggested that similar safe harbour agreements must be concluded between South Africa and some of its other trading partners. Some of these major trading partners include the United Kingdom, the United States, Germany, Italy, Belgium, and Japan, although it would only be foreseen that such an agreement be reached between South Africa and the United States, since the other five do make provision for adequate measures.

Technological advances also have a role to play. Paul Rosenzweig and Alane Kochems[12] explain that technology is both a problem and a solution for the issues posed by enhanced information collection systems. It can facilitate access to and the accumulation of large amounts of data; however, if that access is not properly managed, the information can be misused. When designed with proper procedures and protections and combined with oversight, technology can provide a reasonable balance between security and privacy. They continue by stating that in properly determining how best to enhance both liberty and security, it is useful to have some basic principles for assessing data protection technologies. They contend that such a list might include the following:

- The data protection technology should allow for clear audit tracks to prevent data alteration or identify when data have been changed.
- The technology should have a means to provide graduated levels of access to the data.
- The technology should have protocols for enforcing the confidentiality and security of the data.

There are multiple approaches to securing data. One means is following one of the many published information security standards; another is to protect the most sensitive data through encryption. They conclude by stating that controlling access to data and making sure that entities only have the appropriate level of access is critical if privacy interests are to be protected. Various software companies have adapted its data collection programs to

[8] These countries include Angola, Botswana, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Kingdom of Swaziland, Tanzania, Zambia and Zimbabwe. For further information, see http://www.sadc.int/home.php (24 August 2007)

[9] See http://www.export.gov/safeharbor/ (24 August 2007) for a detailed discussion on the safe harbour agreement.

[10] Ibid note 85.

[11] The objectives of SADC as stated in Article 5 of the Treaty are to: Achieve development and economic growth, alleviate poverty, enhance the standard and quality of life of the people of Southern Africa and support the socially disadvantaged through regional integration; Evolve common political values, systems and institutions; Promote and defend peace and security; Promote self-sustaining development on the basis of collective self-reliance, and the interdependence of Member States; Achieve complementarity between national and regional strategies and programmes; Promote and maximise productive employment and utilisation of resources of the Region; Achieve sustainable utilisation of natural resources and effective protection of the environment; Strengthen and consolidate the long-standing historical, social and cultural affinities and links among the people of the Region.

[12] Their article titled "Data Protection: Safeguarding Privacy in a New Age of Technology" can be viewed at: http://www.heritage.org/Research/HomelandSecurity/lm16.cfm (26 August 2007)

make provision for legislation. A number of academic writers[13] are also of the point of view that the solution would be in the code and that lex informatica could be a useful policy device. But this is a discussion in its own right. The fact that technology would and in fact must play a role is unmistakable and its contributory role in the banking industry could provide solutions to successful implementation of the proposed POPIA.

The last and probably most crucial factor is the facilitation of sector based codes of conduct. Codes offer flexibility and can be adapted to the specific economic, technological and regulatory contexts of different sectors. With or without legislation, codes will continue to be significant instruments by which organisational responsibilities are defined, employee obligations are communicated and citizen rights are established.[14]

In New Zealand, the approach is that codes of practice under its Privacy Act have the force of law. A breach of a ratified code of practice is as serious as a breach of the information privacy principles expressed in the law, which would then trigger the complaints and enforcement procedures in the legislation.[15] Although the Dutch system is similar in most respects to that in New Zealand, the codes are not formally binding on the courts. The proposed POPIA makes provision for codes in its section 62 to be legally binding.

In Australia an organisation or industry registering a Privacy Code under the Australian Privacy Act, must prove and be legally accountable for the Code providing at least the same level of protection that the ten National Privacy Principles of the Australian Privacy Act require – preferably more.[16]

If the proposed POPIA is to follow a co-regulatory scheme as is proposed by the SALRC, then the question has to be asked whether the current industry codes of practice will suffice.

In terms of Section 54(2) (a) of the proposed POPIA, a code of conduct must incorporate all the information protection principles[17] or set out obligations that, overall, are the equivalent of all the obligations set out in those principles[18].

It is generally recognised that five kinds of privacy code can be identified according to their scope of application: organisational code, the sector code, the functional code, the professional code and the technological code.[19]

The approach envisaged by the proposed POPIA seems to be on par with the co-regulatory scheme of Australia where any business or profession may develop a Code of Practice. The code must then be submitted to the Privacy Commissioner for approval. If the Code is deemed to be acceptable then the Commissioner may issue it.[20]

The solution does not necessarily arrive with the issuing of the codes themselves, but rather through a pre-emptive strike and pro-active based effort on behalf of the specific sectors to submit such codes to the Commissioner. If industries sit back and wait for the Commissioner to issue these codes, problems might arise as to the interim position on the implementation and interpretation of the proposed POPIA. Having regard to the specific related problems that might arise from an industry's perspective, courts could create precedents[21],

---

[13] Lessig, Lawrence in "Code and other Laws of Cyberspace", Reidenberg, Joel R. in "Lex Informatica: The Formulation of Information Policy Rules Through Technology", Texas Law Review, University of Texas at Austin School of Law Publications, 76 (3) 1998 pp. 553-584, Rotenberg, Marc in "Fair Information Practices and the Architecture of Privacy" (What Larry Doesn't Get), Stanford Technology Law Review, Cite as: 2001 Stan. Tech. L. Rev. 1 http://stlr.stanford.edu/STLR/Articles/01_STLR_1 (22 August 2007)

[14] Bennett CJ "The Protection of Personal Financial Information: An Evaluation of the Privacy Codes of the Canadian Bankers Association and the Canadian Standards Association" Prepared for the "Voluntary Codes Project" of the Office of Consumer Affairs Industry, Canada and Regulatory Affairs Treasury Board, March 1997 available at http://web.uvic.ca/polisci/bennett/

[15] See Part VI of the New Zealand Privacy Act.

[16] Comments on SALRC draft proposal by Michalsons.

[17] A good example of a code of conduct that incorporates all the information protection principles was the 1996 Canadian Bankers Association Privacy Model Code. See discussion at http://web.uvic.ca/~polisci/bennett/research/cba.htm. (06 August 2007)

[18] A further example of a code of conduct that set out obligations that, overall, are the equivalent of all the obligations set out in those principles is the Netherlands Code of Conduct for the Processing of Personal Data by Financial Institutions.

[19] Project 124, October 2005, Privacy and Data Protection.

[20] See Part IIIA of the Australian Privacy Act 1988 as amended.

[21] See for instance Unitas v Van Wyk & Naude case nr 231/2005. Sec 50 – meaning of "required" for exercise or protection of right – when available to compel pre-action production. The threshold of "required" was set very high due to uncertainty on whether to use

which in the absence of such co-regulatory structures, could be detrimental to the industry as a whole. With its sector based knowledge, it is therefore suggested that the various industries, make sure that they have these codes of conduct or privacy codes ready for submission when the proposed POPIA becomes enacted, thereby annihilating any room for an uncertain interim period that might be subject to scrutiny.

the Promotion to Access of Information Act (PAIA). PAIA was not the appropriate remedy. Discovery would probably have been successful in this delictual action.

# Prevention is Better than Prosecution: Deepening the Defence against Cyber Crime[1]

**Jacqueline Fick**
PricewaterhouseCoopers
Johannesburg, South Africa
jacky.fick@za.pwc.com

## ABSTRACT

In the paper the author proposes that effectively and efficiently addressing cyber crime requires a shift in paradigm. For businesses and government departments alike the focus should be on prevention, rather than the prosecution of cyber criminals. The Defence in Depth strategy poses a practical solution for achieving Information Assurance in today's highly networked environments. In a world where "absolute security" is an unachievable goal, the concept of Information Assurance poses significant benefits to securing one of an organization's most valuable assets: Information. It will be argued that the approach of achieving Information Assurance within an organisation, coupled with the implementation of a Defence in Depth strategy can ensure that information is kept secure and readily available and provides a competitive advantage to those willing to invest and maintain such a strategy.

**Keywords:** cyber crime, cyber law, defence in depth, layered defence, information assurance, information security, public private partnerships, risk management

## 1. INTRODUCTION AND APPROACH

The President in his State of the Nation address on 3 June 2009 specifically referred to an increased effort to combat cyber crime and identity theft.

Cyber criminals in South Africa have increased their attacks in both the private and public sector, with the most prevalent (cyber) offence remaining that of identity theft. However, it must be borne in mind that identity theft is in most cases a means to an end: to assume someone's identity to evade the police, to obtain credit on someone else's credentials where the criminal is not able to do that on his/her own, to gain access to bank accounts, to launder money, etc.

But at the heart of cyber crime in South Africa lies the true asset these criminals wish to obtain: information. Information has become the most important asset any business or government department has and it is this information that enables a criminal to assume another identity, to log into another's bank account, to steal confidential information, to deny an organisation access to its critical information systems. Yet we fail to protect it with the same vigour as we protect our money or property.

Secondly, South African law enforcement has been hampered in effectively dealing with this breed of criminals, due to for example resource constraints and a lack of sufficient training. We also have no accurate statistics to determine the true value of these crimes, nor the extent to which they have harmed our country.

Dealing with cyber crime in South Africa calls for a shift in paradigm: new investigative methodologies and techniques, an increase in effective public private partnerships, better sharing of business intelligence and information and most importantly, moving from a re-active to a pro-active approach to dealing with cyber crime.

[1] A shorter version of this paper was first presented at the Lex Informatica conference held in Johannesburg, South Africa in July 2009. The paper based upon that presentation was then first published in the October 2009 issue of De Rebus, the South African Attorneys' Journal. 

This paper aims to show that prevention is better than prosecution. Devoting time and resources to implement strategies that make it difficult for criminals to perpetrate their crimes within organisations is more efficient and cost effective than trying to catch them after you had been the victim of a cyber attack. And in the unlikely event that you do fall victim to cyber crime and you have the right strategy and systems in place, you would also have a disaster recovery plan in place that enables the organisation to effectively and efficiently deal with the consequences of an attack, an audit trail that can point your investigation in the right direction and evidentiary material available that could stand the scrutiny of a court.

Catching and eventually prosecuting cyber criminals are difficult and costly, both in terms of money, time and resources. For businesses and government alike the reputational damage attached to a cyber attack can also be costly.

The author is of the opinion that implementing the five core principles of Information Assurance and the Defence in Depth strategy, poses significant benefits to the prevention of cyber crime within South African businesses, as well as in government. It will be submitted that the approach of achieving Information Assurance within the organisation, coupled with the implementation of a Defence in Depth strategy can ensure that information is kept secure and provide a competitive advantage to those willing to invest in such a strategy.

## 2. INFORMATION ASSURANCE

### 2.1 Definition

Information Assurance is defined in Wikipedia as the practice of managing information-related risks. More specifically, Information Assurance seeks to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability and non-repudiation. These goals are relevant whether the information is in storage, processing, or transit and whether threatened by malice or accident. In other words, Information Assurance is the process of ensuring that the right users have access to the right information at the right time.

According to the US Department of Defence Dictionary of Military and Associated Words, 2003 Information Assurance is defined as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance is closely related to Information Security and the terms are sometimes used interchangeably. However, its broader connotation also includes reliability and emphasises strategic risk management over tools and tactics. In addition to defending against malicious hackers and code, Information Assurance includes other corporate governance issues such as privacy, compliance, audits, business continuity and disaster recovery. Whilst Information Security draws primarily from computer science, Information Assurance is interdisciplinary and draws from multiple fields, including accounting, fraud examination, forensic science, management science, systems engineering, security engineering and criminology, in addition to computer science.

Information Assurance can be viewed as an umbrella concept bringing together issues of information security and dependability. It must always be borne in mind that “absolute security” is an unachievable goal. What the concept of Information Assurance proposes is defined in its name: it is providing organisations with an acceptable level of assurance that even when there are attempts to interfere with the security, availability and reliability of networks and systems, there will still be an acceptable level of functionality.

### 2.2 Objective of Information Assurance

The objective of Information Assurance is to minimise the risk that information systems and the information stored, transmitted and processed thereon is vulnerable to threats. This implies that, if an attack does take

place, the damage it might cause will be minimised. It also provides for a method to recover from the attack as efficiently and effectively as possible.

Information Assurance requires an organisation to focus on its access controls (both physical and logical access controls), individual accountability to ensure that each user of the system can be identified and to provide for audit trails which can provide historical records when a system is compromised.

### 2.3 Five Pillars of Information Assurance

Information Security is based on what is known as the CIA triad, namely confidentiality, integrity and availability. Information Assurance has an additional two principles namely authenticity and non-repudiation. Together they form the so-called five pillars of Information Assurance.


Figure 1: The five pillars of Information Assurance

The National Security Agency of the United States of America (NSA) recommends that the application of the five pillars of Information Assurance should be based on the Protect, Detect and React paradigm. This means that in addition to incorporating protection mechanisms, organisations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks. It further recommends the implementation of a Defence in Depth strategy to achieve Information Assurance. This strategy will be discussed in full below.

Upon analysis of the Electronic Communications and Transactions Act, No. 25 of 2002 (ECT Act), it becomes clear that the five pillars of Information Assurance is entrenched in our legislation and that in most instances, a breach in any of these areas has been criminalised.

#### *2.3.1 Confidentiality*

Keeping information confidential implies that information must only be accessed, used, copied or disclosed by users who have been duly authorised to do so. This would include for example where you allow someone to only view information and not copy it for them, but the person was not authorised to see the information in the first instance.

In terms of section 85 of the ECT Act "access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data. Section 86 of the ECT Act criminalises the unauthorised access to, interception of or interference with data.

In terms of section 86(2), read with section 89(1) a person who intentionally accesses or intercepts data without the authority or permission to do so is guilty of an offence and is liable to a fine or imprisonment not exceeding twelve months.

#### *2.3.2 Integrity*

Data integrity also deals with authorisation and implies that data may not be created, altered or deleted without

the proper authorisation. A loss of integrity could occur when a computer is infected with a virus, or where someone gains unauthorised accesses to a server and deletes critical data files. Data integrity is also important in cases where computer evidence is to be used in court.

In terms of section 14(1) of the ECT Act, where the law requires that information is to be presented or retained in its original form that requirement is met by a data message if the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment and that information is capable of being displayed or produced to the person to whom it is to be presented.

In terms of section 14(2) the integrity must be assessed by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display, as well as in light of the purpose for which the information was generated and having regard to any other relevant circumstance.

Section 17 stipulates that where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document, as well as that at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference. Section 17(2) furthermore provides that the integrity of the information in a document is maintained if the information has remained complete and unaltered, except for the addition of any endorsement, or any immaterial change, which arises in the normal course of communication, storage or display.

Section 86(2), read with section 89(1) of the ECT Act provides that a person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence and is liable for a fine or imprisonment of up to twelve months.

### *2.3.3 Authenticity*

In simple terms authenticity means that a user that logged on to a computer is in reality the person whose credentials (e.g. user name and password) was used, or that documents on a computer have not been altered or forged.

The most common authentication breach in South Africa is where user id's and passwords are stolen (identity theft) and used to load false transactions on a system. One must always bear in mind that identity theft is not when someone steals your credit card number, it is when someone steals *you* (Campana, 2006).

According to Scott Charney from Microsoft (Tung, 2008) much has been done in terms of defence in depth against malware or against phishing schemes, but more remains to be done. For this to happen, better authentication is required so that users can make better decisions about what is running on their computers. Charney also noted that there has been a major shift by software vendors to tie software more tightly to hardware to solve the problem of authentication. According to him one needs operating systems that are bound to the hardware, so that if it is tampered with there is better chance of knowing about, detecting and remediating the problem.

Chapter VI of the ECT Act provides for the authentication of service providers in South Africa where accreditation is defined as the recognition of an authentication product or service by the Accreditation Authority. Authentication products or services are defined as products or services designed to identify the holder of an electronic signature to other persons.

In terms of section 86(3), read with section 89(1) a person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs

any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence and liable to a fine or imprisonment not exceeding twelve months.

Section 86(4), read with section 89(2) furthermore provides that a person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence and liable to a fine or imprisonment not exceeding five years.

### *2.3.4 Availability*

Availability does not only mean that the information on a system must be readily available, but also that the systems needed to process the information and the security measures that protect the information are all functioning properly at the time the information is needed. In simple terms the right information must be available to the right person at the right time.

During a denial of service (DoS) attack, information is not readily available because the users cannot access the information on their computers. Section 86(5) of the ECT Act, read with section 89(2) provides that a person who commits any act with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial of service to legitimate users is guilty of an offence and liable to a fine or imprisonment not exceeding five years.

### *2.3.5 Non-repudiation*

Non-repudiation implies that parties to an electronic transaction are bound in terms of that transaction: the one party cannot deny having received the information, nor can the other party deny sending it.

In terms of section 25 of the ECT Act a data message is that of the originator if it was sent by the originator personally, or by a person who had the authority to send it on behalf of the originator, or if it was sent by an information system programmed by or on behalf of the originator to operate automatically, unless it is proved that the information system did not properly execute such programming.

An acknowledgement of receipt of a data message is not necessary to give legal effect to the message, but in terms of section 26 of the ECT Act acknowledgement of receipt may be given by any communication by the addressee, whether automated or otherwise, or any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

In terms of section 23 of the ECT Act a data message used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee. It is also stated that a data message must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee, and must be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence.

In electronic commerce digital signatures are commonly used to establish authenticity and non-repudiation. Section 13 of the ECT Act stipulates that where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.

## 3. DEFENCE IN DEPTH STRATEGY

### 3.1 Introduction

Due to the rapid development of business, IT trends and technology, it has become increasingly important to maintain proper control of an organisations' information. It is now commonly recognised that information is one of (if not) the most valuable assets an organisation has. This information pertains to various business

processes and disciplines within a single organisation: ranging from strategic management information to basic operational process information.

Defence in Depth is a strategy that can be implemented to achieve Information Assurance in today's highly networked environments. According to the NSA it is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy is based on balancing protection capability and cost, performance and operational considerations.

In its report on Defence in Depth, the Trusted Information Sharing Network (TISN) defines Defence in Depth as the systematic security management of people, processes and technologies, in a holistic risk-management approach.

The concept is based on military strategy which implements defences primarily to delay rather than prevent the advance of an attacker. It is assumed that an attack will lose momentum over time, allowing for those being attacked to respond appropriately. This strategy is particularly useful when dealing with Information Assurance as one can never rule out the possibility of an attack, but one can implement a strategy that effectively and efficiently guards against, monitors and reports on such attacks and, in the event that an attack does take place provides for a strategy to address the damage.

According to the TISN (TISN, 2008) the Defence in Depth is far more than an IT concept, as it delivers:

- effective risk-based decisions;
- enhanced operational effectiveness;
- reduced overall cost and risk; and
- improved information security.

Defence in Depth provides an approach to security that is integrated with the organisation's business processes and enterprise-wide risk management capability.

For an organisation to effectively protect its information and information systems against cyber attacks, it is necessary to determine who the enemy is, why they would want to launch an attack against the organisation and how they would then attack the organisation.

Threats to the confidentiality, integrity and availability of an organisation's information assets can arise through its employees, business partners, external sources and technological innovation. The potential cyber criminal might be a disgruntled employee that aims to commit corporate espionage or launch a denial of service attack, or it might be a cyber syndicate that wants to steal user id's and passwords to gain access to your client's bank accounts. Threats can also relate to intentional and unintentional actions that can potentially harm information assets. Examples of these threats include the following (TISN, 2008):

| **PEOPLE** | **TRADING PARTNERS** |
|---|---|
| • Disgruntled employees<br>• Financially troubled employees<br>• Corporate espionage<br>• Uneducated/uninformed users | • Business partners with poor data security<br>• Physical access to shared systems<br>• Misunderstanding of allowed access<br>• Competitive environment |
| **EXTERNAL THREATS** | **TECHNOLOGICAL INNOVATION** |
| • Hackers<br>• Organised crime<br>• Changes in regulatory framework | • Faster networks<br>• More storage in smaller devices<br>• Technological convergence<br>• Increasingly mobile workforce |

### 3.2 Focus Areas of Defence in Depth Strategy

An important principle of the Defence in Depth strategy is that achieving Information Assurance requires a balanced focus on four primary elements, namely People, Technology and Processes (or Operations) and Governance.

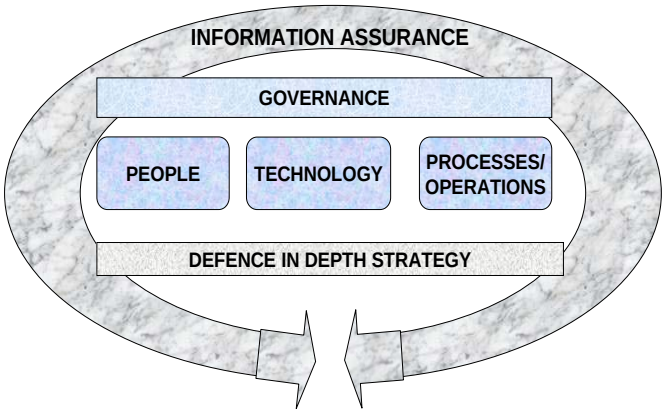


Figure 2: People, Processes, Technology and Governance

Figure 2 outlines the basic principles of a Defence in Depth strategy. The strategy is based on the concepts of technology, people and processes (or Operations), and governed in terms of a management framework.

Furthermore, it is of paramount importance to determine what the organisations' system priorities are. In other words which systems are critical to business operations and are needed to ensure operational effectiveness and a competitive advantage?

#### *3.2.1 Technology*

Technology refers to solutions that organisations employ that enable them to achieve and sustain their business objectives. Key focus areas for implementing a Defence in Depth strategy in terms of technology would include the management of network architecture, infrastructure management, application security and communications management.

A wide range of products are available that provide for Information Assurance services and detecting intrusions. It is, however, of paramount importance to ensure that the organisation's procurement policy is aligned to the overall Defence in Depth strategy and that the right technology is procured in accordance with the achievement of overall business objectives. An effective procurement policy and process must have regard to the organisation's security policy, what level of security is needed for a particular application, if the particular product has been validated by a reputable third party, a risk analysis pertaining to the acquisition of the particular technology or product, issues of integration with current systems and processes, etc.

#### *3.2.2 People*

Within the context of the Defence in Depth strategy People refers to the security roles and responsibilities for internal and external persons. It is essential to define, maintain and enforce security roles and responsibilities for employees within the organisation, contractors or business partners that the organisation deals with, service providers that are used where functions are outsourced and service providers that supply products or services to the organisation.

Another key focus area would be user awareness and ensuring that all relevant internal and external persons are fully aware of and conversant with their particular role and responsibility and the procedural and governance framework, as well as policies applicable to them.

### *3.2.3 Processes (or Operations)*

Processes (or Operations) refer to the standardised actions which are used to ensure the organisation's position on security is sustained. What this means in terms of the Defence in Depth strategy is that organisations must define, maintain and enforce standardised actions/processes which are used to develop and sustain its position on security on a daily basis.

Key focus areas for the implementation of the strategy would typically include identity and user-access management, incident response management, disaster recovery management and audit management.

The NSA provides the following examples of activities that are traditionally categorised under this heading:

- Maintaining a visible and up to date system security policy.
- Certifying and accrediting changes to the Information Technology baseline. These processes should provide the data to support risk management-based decisions. It should also acknowledge that a "risk accepted by one is a risk shared by many" in an interconnected environment.
- Managing the security posture of the Information Assurance technology (e.g. installing security patches and virus updates and maintaining access control lists).
- Providing key management services and protecting the relevant infrastructure.
- Performing system security assessments, e.g. vulnerability scanners to assess the continued "security readiness" of the organisation.
- Monitoring and reacting to current threats.
- Attack sensing, warning and response.
- Recovery and re-constitution.

### *3.2.4 Governance*

Within the context of a Defence in Depth strategy, governance refers to the oversight and coordination of technology, people and processes that is provided in terms of a management framework. Key focus areas for the implementation of the Defence in Depth strategy would include risk management, information security and policy and compliance management. Achieving Information Assurance through a Defence in Depth strategy would traditionally begin with commitment from a senior management level (such as from the Chief Information Officer), based on a clear understanding of exactly what the threats are that the organisation is facing. This is then followed up by integrating and aligning the understanding with the organisation's overall strategy, aligning with and incorporating it into with the business objectives and goals, drafting and implementing appropriate policies and deriving suitable procedures from them.

## 3.3 Core Principles of Defence in Depth Strategy

The TISN (TISN, 2008) defines the core principles of a Defence in Depth strategy as follows:

- Implementing measures according to business risks.
- Using a layered approach which would mean that if a single control fails, it would not result in the whole system being compromised. The concept of a layered approach or layered defence is discussed under paragraph 3.5.
- Implementing controls in such a way that they would increase the effort needed to attack and breach the system.
- Implementing personnel, procedural and technical controls.

In order to successfully implement a Defence in Depth strategy management must include the core principles of this strategy in the organisation's overall strategy, in their annual planning, as well as within their organisational structure.

It is important that the Defence in Depth strategy should not only protect against attacks, but also enable organisations to detect attacks and effectively respond to it. It must also be borne in mind that attacks can take place from multiple locations by people from both inside the organisation or by outsiders. It would therefore be necessary to deploy controls at multiple locations to guard against all classes of attacks.

A further important consideration is that, in case of an attack happening within an organisation, the audit trail must be of such a nature that it would assist the organisation in taking appropriate internal disciplinary steps or that they would be able to provide sound evidentiary material and assistance to law enforcement agencies where criminal proceedings are to be instituted.

### 3.4 Implementing a Defence in Depth Strategy

Implementing a Defence in Depth strategy requires a shift in paradigm. Organisations must move away from the notion that IT security and/or Information Assurance are stand-alone issues, to where these concepts become an integral part of business planning, overall strategy, governance and operations.

If one were to explain in practical terms what the importance of achieving Information Assurance is, try to imagine any organisation functioning without IT systems and support and even more pertinently, how any organisation can sustain its proper functioning and competitive advantage without securing, preventing unauthorised access to and insuring availability and functionality of its critical information.

According to the 2009 IDG Research Services Survey some companies are so enthusiastic about the potential of new web and mobile technologies that they deploy them without adequately securing critical processes and data. Implementing a Defence in Depth strategy requires co-ordinating and integrating knowledge of the overall strategy and goals of the organisation or department, the internal environment (including systems, personnel and information assets), and the internal and external threat environment.

The TISN (TISN, 2008) have identified four reasons why it is necessary to implement a Defence in Depth strategy:

- **Expanding organisational boundaries**: Businesses today form close alliances with their business partners, customers and suppliers. This results in hard-to-define external boundaries, for example where business partners form a consortium to deliver a product, it might be that they rely on the same infrastructure, IT systems, personnel, etc. to deliver the specific product. There is a need to determine where the organisations' boundaries lie and what it is that it aims to protect by implementing a Defence in Depth strategy.
- **Mobile workforce**: It has become increasingly important for employees to be able to access their company networks from a remote location. Employees need to access their emails from home or have their mail delivered to a Blackberry device. The close interconnectivity between controls and office networks enable viruses and worms to spread more easily to control systems (Lüders, 2006).
- **Decentralisation of services**: As the use of computers in the workplace increases, so does the provision of services and systems via the intra and extranets. Previously it was only necessary to grant access to a select few, but these services and systems now have to be provided to a broader set of users.
- **Increasing value of information**: As stated above, businesses have realised what the value of information is to maintaining and sustaining a competitive advantage. Due to the value of information, it has become increasingly important to apply stringent security measures to guard against the loss, destruction, tampering and theft of a businesses' information. It is also important to ensure that the right person has the right access to the right information at the right time.

The steps to implementing a Defence in Depth Strategy can be summarised as follows:

- **Analysis of internal and external environment**: The first step towards implementing a Defence in Depth strategy would be to analyse the internal and external environment in which an organisation operates: what its strengths and weaknesses are, the threats the organisation faces, what systems, assets, technology and processes are being used? It is also necessary to establish what the organisations' overall strategy is, to determine if the Defence in Depth strategy is aligned to business objectives and goals and if there is a clear understanding of what the Defence in Depth strategy means for the organisation, as well as what it would entail to implement it.
- **Determining the risks**: The second step is to determine what risks the organisation faces (in terms of Information Assurance): based on the weaknesses, threats and vulnerabilities that have been identified it is necessary to firstly establish if the organisation is aware of the identified risks and if they understand the implications of such risks. The identification of risks and proposing of mitigating actions must always be done in light of the particular organisations' risk appetite.
- **Implementation of Defence in Depth strategy**: Once all risk areas have been identified and mitigation plans proposed, it is necessary to implement the proposed controls in such a way that it ensures optimum functionality of systems, the integration of controls across the organisation, as well as compliance with the overall business strategy and risk management process.
- **Maintenance, monitoring and review**: Due to the fast changing environment of IT, it is necessary to continuously monitor and review the functioning of the strategy, to adapt it to any changes in threats the organisation might face, changes to business goals or objectives or changes to the regulatory environment.

### 3.5 Layered Defence Approach as part of Defence in Depth Strategy

Modern trends place increasing demands on information security within an organisation: users need remote access to the network, third parties have to access the organisation's network to perform certain functions or access specific information and more users within the organisation now need access to resources that were previously granted to a select group of users.

The most effective way to secure information within these parameters would be through implementing different layers of control as part of the Defence in Depth strategy (Murali et al., 2007). Tippett (2004) warned that "perfection in information security is impossible" and that smart people should zero in on identifying and building layered security controls around the network, because layering meant that even if one control failed, another was almost certain to catch the problem.

Webopedia defines a layered defence as multiple layers of protection. A layered defence means having multiple barriers to prevent attack, infiltration or malware infestation. These may include malware protection, possibly from multiple vendors, running at web and email gateways as well as on the desktop, firewalls at the network edge and on endpoints, intrusion detection, system intrusion detection systems and behavioural monitors, data leak prevention systems and a wealth of other possible defences, all operating in harmony to provide best-possible protection.

Controls will generally include both technical and process control mechanisms. Figure 3 provides a graphical representation of the layers of control implemented around a business process or key piece of business information (TISN, 2008):

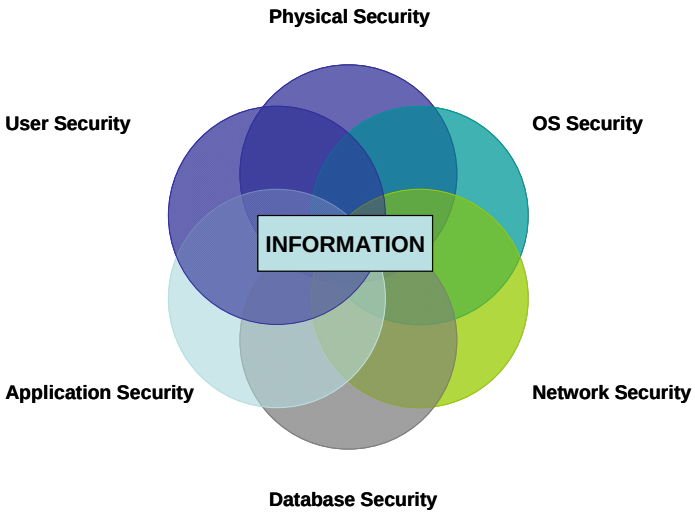


Figure 3: Layered Controls

Within the context of a Defence in Depth strategy a layered defence would mean that an organisation deploys multiple defence mechanisms between the attacker and the target. Each of the mechanisms must present its own unique obstacle to the attacker and must also include both protection and detection measures.

In practical terms it must increase the difficulty of successfully penetrating the network and thereby reducing risk, but also at the same time increase the chances of detecting the intruder:

- It must identify users of a system by means of passwords, user names, etc.
- It must also be able to provide for mechanisms to effectively and efficiently recover from damage caused by an attack.
- It must also be possible to correlate the results of information from various departments within a business and information from different controls, in an effort to increase business intelligence that can be used to identify and prevent future attacks and that can be shared within the market or with law enforcement agencies.

Within a broader context the concept of layered defence can also refer to the combined efforts of the public and private sector to combat cyber crime. The most powerful weapon available to fight cyber criminals is the very same asset they seek: information. Cyber criminals often rely on businesses, government and law enforcement not sharing any information or connecting random attacks to establish a *modus operandi*. They are often able to strike at different businesses within a same industry within a relative short period of time, because businesses are reluctant to share information about attacks with their counterparts. Although this is understandable seen in light of the fact that businesses might loose competitive advantage or market share, it is only the criminals that benefit from not sharing information about attacks.

However, the more developed the methods of information sharing between industry members, and between business and law enforcement agencies are, the less the need for a situation where full public disclosure will be called for.

### 3.6 Maintaining a Defence in Depth Strategy

Maintaining a Defence in Depth strategy includes continuous monitoring and evaluation of the effectiveness of the implemented program. This would include evaluation the strategy to determine alignment where there are changes to the organisations' business objectives or the overall enterprise strategy, where there are changes in the security profile or specific breaches in security occur, where there is an increase in particular security breach phenomena such as an increase in key loggers that are being detected throughout the industry, as well as when weaknesses or gaps that are identified within the current strategy.

The TISN (TISN, 2008) also recommends the model outline in Figure 4 to analyse the combined effectiveness of individual protection layers – whether currently in place or proposed for implementation. The effectiveness of these individual protection layers must then be considered within the context of the identified threat environment.

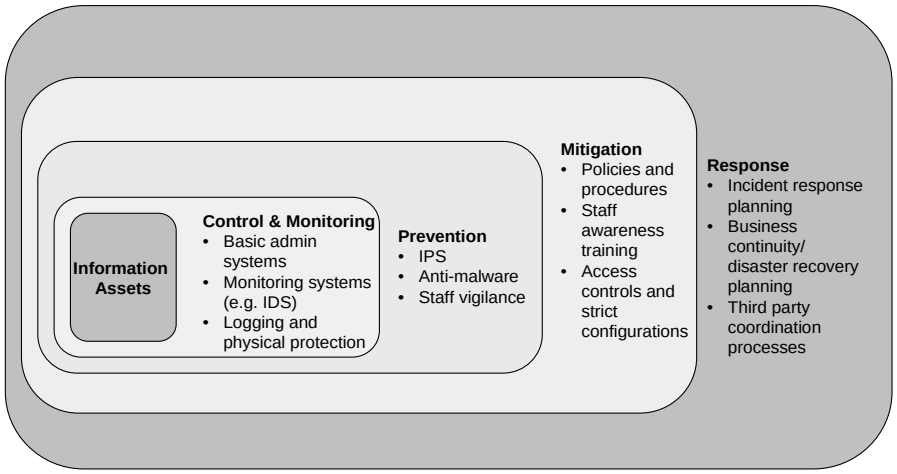


Figure 4: Layers of control protecting an information asset (TISN, 2008)

Practical guidelines for maintaining the strategy and improving on it where applicable can include the following:

- **Know and understand your organisation**: This includes an understanding of the external environment and the threats facing the organisation. It also refers to a thorough understanding of the internal environment and the way the organisation operates – its employees, levels of staff morale, business partners of the organisation, service providers, etc.
- **Define security roles and responsibilities**: Although security should be everyone within an organisation's concern, ownership of information security should be assigned to specific individuals, coupled with the necessary levels of authority and accountability. To assist with the process it is recommended that security roles and responsibilities be incorporated into job description and that performance in terms of these areas be measured accordingly.
- **Adopt appropriate policies and procedures**: Once the Defence in Depth strategy has been drafted, the necessary policies and procedures should be put in place to govern the proper use of IT within the organisation, thereby ensuring optimal security. This would include updating policies and procedures as the need arises and to incorporate necessary changes in regulations, technology or operational requirements, as well as training and the creation of awareness with internal and

external users. It is also critical to develop and define an appropriate incident response procedure and that this procedure is communicated to all users.

- **Continuous auditing and assessment of process**: It is recommended that a process of continuous auditing be implemented to ensure that the strategy remains aligned to business objectives, adapts to changes in technology or identified threats, and to allow for the analysis of information that is gathered from the different implemented controls.
- **Stay up to date**: Maintain awareness of new developments in both technology and services. Use a risk-based approach to determine when it would be necessary to upgrade or adapt current systems and processes to accommodate new developments.
- **Effective public private partnerships**: The effective control of cyber crime requires more than just cooperation between public and private security agencies. The role of the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation is also of critical importance. To effectively address cyber crime also calls for a less re-active and more pro-active approach to the prevention, detection, investigation and prosecution of these crimes. Whilst it might be that only law enforcement can arrest criminals, service providers and private sector organisations can do much to investigate and prevent cyber crime (Forman, 2009). Within the context of a Defence in Depth strategy, such partnerships can deliver valuable business intelligence to prevent further attacks or to be able to detect them within an information system. Criminal intelligence analysis needs to be integrated fully into business intelligence, risk assessment needs to incorporate criminal threats, and cyber security needs to be conceptualised as part of a broader security problem that cannot be understood or dealt with in strictly technical terms (Williams, 2009).

## 4. CONCLUSION

In today's world information is fast becoming the most valuable asset an organisation has. Information underpins every strategy, system and business objective within an organisation and without ready and reliable access thereto, organisations cannot function on an optimal level.

It is however, critical to preserve the integrity of information, to ensure that it is stored, transmitted and accessed securely and that any system designed to manage and secure information is reliable, aligned to business objectives and in accordance with the risk management approach of the organisation.

Achieving Information Assurance in an organisation through the implementation of a Defence in Depth strategy poses significant benefits. It also ensures that South African organisations are aligned to the regulatory provisions contained in the ECT Act.

The shift in paradigm from a re-active to a pro-active approach and focusing on prevention rather than the prosecution of criminals that attack your system, poses benefits in terms of cost, time, resources and organisational reputation. The shift in paradigm required also includes to the need for sharing business (and criminal) intelligence and forming effective public private partnerships, reporting on threats and attacks and balancing what is best for the organisation with what is best for the community as a whole.

## ABOUT THE AUTHOR

Jacqueline Fick is admitted as an advocate of the High Court and holds the degrees B Iuris, LL B and MBA. She has over twelve years' experience as a prosecutor and was legal and strategic advisor to the Head of the Directorate of Special Operations for almost two years. She has presented papers at local and international conferences and is currently employed by PricewaterhouseCoopers in their Advisory Division.

**REFERENCES**


1. Campana, J. (2006), Identity Theft: More than Account Fraud. What everyone should know (April 2006), http://www.jcampana.com,
   accessed on 16/02/2009
2. Foreman, M. (2009), Combating terrorist financing and other financial crimes through private sector partnerships, http://www.emeraldinsight.com/1368-5201.htm,
   accessed on 03/03/2009
3. Lüders, S (2006), A 'defence-in-depth' strategy to protect CERN's control systems (09/02/2009), http://cerncourier.com/cws/article/cnl/24162,
   accessed on 01/07/2009
4. Murali, D and Ramesh, C. (2007), Pseudo-intellectualisms continues to be attached to computer crimes, The Hindu, 04/07/2007, http://www.thehindubusinessline.com/2007/07/05/99hdline.htm,
   accessed on 15/06/2009
5. National Security Agency of the United States of America (NSA), Defence in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments, (date published unknown), http://www.nsa.gov/ia/_files/support/defenceindepth.pdf,
   accessed on 10/06/2009
6. Tippett, Peter (2004), Easy does it, (24/02/2004),
   http://www.computertimes.asiaone.com.sg/people/story/0,5104,2021,00.html,
   accessed on 01/07/2009
7. Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) (2009), Defence in Depth: Summary Report for CIO's and CSO's, (June 2008), http://www.tisn.gov.au,
   accessed on 10/06/2009
8. Tung, L. (2009), Microsoft: Defence in Depth is not enough, (19/05/2008) http://www.zdnet.com.au,
   accessed on 12/06/2009
9. Wikipedia, (2009), Information Assurance, http://en.wikipedia.org/wiki/Information_assurance,
   accessed on 18/06/2009
10. Wikipedia, (2009), Defence in Depth, http://en.wikipedia.org/wiki/defence_in_depth,
    accessed on 18/06/2009
11. Williams, P. (2009), Organised Crime and Cyber-crime: Implications for Business,
    http://www.cert.org/archive/pdf/cybercrime-business.pdf,
    accessed on 13/02/2009

# Telecommunications Liberalisation in Africa: Proposed regulatory model for the SADC region

**Z. Ntozintle Jobodwana**
Department of Public, Constitutional and International Law
College of Law
University of South Africa
E-MAIL: Jobodzn@unisa.ac.za

## ABSTRACT

The liberalisation of the telecommunication industry in Africa, and the further development of the region's physical infrastructure was accompanied by the further development of Africa's information, communication and technology infrastructure. Competition within the industry stimulated heavy economic investment in other sectors of the economy. The outcome of liberalisation also included the establishment of community-based structures that continue to enable communities to manage their own development and gain access to information and communication technologies (ICTs) in an unprecedented manner. The telecommunication infrastructure further stimulated the fast development of other related services, for example, e-commerce and mobile commerce (m-commerce), e-government, internet banking, mobile banking etcetera. Latest reports and statistics disclose that in Africa m-commerce is set to even overtake the development of e-commerce, through the popular use and penetration of mobile telephony whilst e-commerce development is constrained by difficulties in rolling out speedily fixed telephone lines. These new methods of communication have so intensified that there is hope that further penetration of mobile telephony would leap-frog economic growth and development in Africa, especially in rural communities. Therefore, innovations and investment in ICT's are changing the world in a number of ways, resulting in a globally connected digital economy. However, there are regulatory challenges that need to be addressed as a matter of urgency. Certain sections of the continent's population, especially those in rural areas, have very limited access to ICT's. This prevents them from exploiting opportunities offered by ICT's. The main barriers to ICT access relate to inadequate regimes and their supporting legal frameworks, high cost of internet access, connectivity problems, the lack of technical skills to support maintenance and low number of computers with internet connectivity at schools, libraries and other public places. In this paper such challenges are identified and further reforms suggested. The ultimate recommendation is the one that states that a SADC telecommunication independent regulatory agency be established, independent of any government ministry, though consulting with a SADC Ministerial Council. Already, some countries in West Africa have developed a harmonized regulatory framework designed to integrate the Acts covering ICT markets in the sub-region and to keep policy and regulatory frameworks in line with the constant evolution of technologies, applications and services.

## 1. INTRODUCTION

The information communication technologies (ICTs), have become enablers of change though on their own do not create transformation but can best be seen as facilitators of change, innovation and creativity. The most important economic impact of the spread and use of ICTs is indirect and is through transforming the way individuals, business and other parts of the society work, communicate, and interact. In other words, ICTs unleash the creative potential embodied in people. Apart from the contribution the ICTs industry makes to economic growth and development, it also acts as a catalyst in promoting qualitative improvements in other sectors of the economy. Reasons for that are that ICTs are generally important intermediates in production and in the infrastructure on which the information age is being built. It is therefore contended that for Africa, ICTs definitely have the potential to strengthen economic growth and to be used to create new markets, new technological applications for

collaboration, and new methods and tools for scientific and technological research. The ICTs not only facilitate information exchange, but actually deepen the change process, creating new modes of sharing ideas, and reducing the costs of collecting and analyzing information. ICTs are about information flowing faster, more generously, and less expensively throughout the planet. As a result, knowledge is becoming an important factor in the economy, more important than raw materials, capital, labour, or exchange rates. Report of the Commission for Science and Technology for Development (2003) states that "ICTs refer to technologies people use to share, distribute, gather information and communicate, through computers and interconnected computer networks. They are a complex and varied set of goods, applications and services used for producing, distributing, processing, transforming information, including telecoms, TV and radio broadcasting, hardware and software, computer services and electronic media." The present attitude of Africa's governments to the ICT industry has since changed. There is a growing consensus that national monopolies have become inefficient, costly, and sometimes corrupt and therefore must ultimately be opened to private competition if the industry is to flourish. Overall, the consensus seems to be that properly used ICTs could reduce poverty; empower people; build capacities, skills and networks; inspire new governance mechanisms and reinforce popular participation at all levels. The range of applications seem limitless; from electronic commerce (e-commerce), mobile commerce (m-commerce), to the empowerment of communities, women and youth; from the promotion of good governance and decentralization, to advocacy programmes, including the observance of human rights; from long-distance education to tele-health and environmental monitoring.

The process of liberalisation is now being pursued within the World Trade Organization's General Agreement on Trade and Services and Annexures thereto. Building the required infrastructure is a daunting problem in Africa, but these challenges, under an appropriate regulatory regime, can be turned around into opportunities. Business players and stakeholders in the telecommunications industry are generally well-resourced multinational companies which are notorious for using their dominant economic influence to undermine the natural development of infant industry. It is for this reason that in this paper a proposal is made for the establishment of a strong independent, effective, efficient, and well-funded communications regulatory authority for the Southern African Development Community (SADC), as a basis and pioneer for a continental similar project. The aim is to have a regulatory regime that will monitor and coordinate the activities of economic players and protect consumers and weak government alike. A catalyst for economic stability, levelling of the playing ground, providing an environment conducive to investment, and helping governments and other stakeholders manage their ICTs.

Section 1 is a brief discussion of the WTO framework on rules and regulation that guide the service industry, especially the telecommunications sector. Section 2 is a brief survey and an account of progress in the liberalization of the telecommunications sector in Africa and, generally, the dismantling of State monopoly utilities. Privatization issues are also raised and analysed. The future role of mobile telephony industry is particularly included in Section 3, because of its advantages over fixed telephone lines which are costly to roll-out in a continent known for its rugged terrain. Besides mobile telephony has overtaken fixed lines in Africa, and its penetration is fast growing, even reaching out to remote rural areas. In section 4, the competitive environment is analysed more especially as it is influenced by the presence and operation of foreign corporate groups. Concerns have been expressed about their influence and likely dominance in an industry that is capital intensive and employs highly skilled personnel. Section 5 represents the ultimate recommendation of this paper, the establishment of a SADC Communications Regulatory Authority – SADC-CA. Section 6 is the Conclusion.

## 2. THE TELECOMMUNICATION INDUSTRY: THE WTO CONTEXT

The liberalisation processes in the telecommunications cannot just take place outside the WTO framework in terms of the General Agreement on Trade in Services (GATS). Of special importance are the second and third preambular paragraphs of GATS which state:

> *Wishing* to establish a multilateral framework of principles and rules for trade in services with a view to the expansion of such trade under conditions of transparency and progressive liberalization and as a means of promoting the economic growth of all trading partners and the development of developing countries;
>
> *Desiring* the early achievement of progressively higher levels of liberalization of trade in services through successive rounds of multilateral negotiations aimed at promoting the interests of all participants on a mutually advantageous basis and at securing an overall balance of rights and obligations, while giving due respect to national policy objectives …

The trade in services falls broadly into four categories under the WTO umbrella:[1] those services which are supplied across national borders, those services consumed abroad; those services for which a commercial presence is required, and those provided through the presence of a natural person. The dramatic rise in trade in all of these categories since the establishment of the World Trade Organization (WTO) reflects liberalisation in capital markets and freeing of restrictions on capital flows which have increased the ability of large multi-national corporations to enter countries and provide services directly.[2]

Before this development, and in telecommunications industry, all the three standard forms of international growth, i.e. exporting, direct foreign investment and non equity agreements, were barred for a long time by the institutional set up of national markets of this industry.[3] Even international telecommunications were treated as an extension of domestic telecommunications with tight heavily regulated international oligopoly established.[4] As observed by Antonelli, the network of each country was managed just by one firm, heavily regulated, and most importantly, with a strong "national" character. Cristiano Antonelli further states that in almost all the States representing developed or developing countries, telecommunications services were managed either by state-owned companies or directly by public agencies.[5] Today what was once a regulatory area, the telecommunications industry has become a market access issue under the GATS and the General Agreement on Tariffs and Trade. This also, increasingly reflects technological advances in the easy provision of services across borders.

Part II of the GATS establishes the general obligations and disciplines to be observed by all WTO member states.[6] Amongst those likely to have a direct impact on telecommunications regulatory regimes are the following:

- MFN—most favoured nation treatment which is established in Article II,
- legal and regulatory transparency as required by Article III,
- impartial regulation and access to procedures for review under Article VI,
- the obligation under Article IX to work toward the elimination of business practices that may distort competition, and
- the obligation on members to enter into negotiations regarding subsidies.

---

[1] See Angus Henderson, Iain Gentle & Elise Ball, 'WTO Principles and Telecommunications in Developing Nations: Challenges and Consequences of Accession' 29 (2005) *Telecommunications Policy*, 205–221

[2] See generally Cristiano Antonelli, 'Technological Change and Multinational Growth in International telecommunications Services', 10 *Review of Industrial Organization,* 161-162.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] See Bobjoseph Mathew, *The WTO Agreements on Telecommunications* (2003) , 81-82.

Countries make specific commitments, limitations and conditions pursuant to Part III of GATS, in respect of market access,[7] national treatment,[8] and additional commitments.[9] It is particularly in terms of Articles XVI and XVII that specific commitments are made by countries in the telecommunications sector in relation to the opening of competition and issue of additional licences (market access) and foreign investment (national treatment), respectively.

GATS was initially opposed by most governments in the developing countries, as there was a perception that in future there would be dramatic increase in the provision of often essential services by foreign entities.[10] These fears were justified on several grounds, amongst which were, that any such agreement would threaten the right of governments to maintain public services, that liberalisation of services markets under the WTO would effectively mean deregulation, and that foreign investment in the supply of services would retard the development of the relevant infant local service industry. The developing countries had argued that in the service industry sector, developed countries were already enjoying comparative advantage over developing countries, in a service industry sector which was capital intensive needing highly skilled personnel.[11] Obviously, in view of the fact that the governments of developing countries typically face tight fiscal constraints, there was fear about the dissipation of revenues through foreign competition.

According to the World Trade Organization, the telecommunications services are a global market worth over US$ 1.5 trillion in revenue.[12] The participation of African countries, especially, the least developed countries (LDCs), in this sector is very crucial as it has foreign direct investments implication in billions of US dollars. The mobile services account for roughly 40 per cent of this market, while mobile subscribers worldwide currently outnumber the use of fixed telephone lines by more than two to one.[13] Since 1998, the market has witnessed far-reaching changes, with the introduction of competition into a sector that was once principally a monopoly.[14]

Commitments in telecommunications services were first made during the Uruguay Round (1986-94), mostly in value-added services. In post-Uruguay Round negotiations (1994-97), WTO members negotiated on basic telecommunications services. Since then, commitments have been made by new members, upon accession to the WTO, or unilaterally at any time. According to the WTO report, a total of 108 WTO members have made commitments to facilitate trade in telecommunications services.[15] These commitments include the establishment of new telecoms companies, foreign direct investment in existing companies and cross-border transmission of telecoms services. Out of this total, 99 members have committed to extend competition in basic telecommunications (e.g. fixed and mobile telephony, real-time data transmission, and the sale of leased-circuit capacity).[16] In addition, 82 WTO members have committed to the regulatory principles spelled out in the "Reference Paper", a blueprint for sector reform that largely reflects "best practice" in telecoms regulation.[17]

Telecommunications, like other services, are included in the services negotiations, which began in January 2000. In the current Doha Round of negotiations, additional market opening as well as the binding of recent reforms (i.e. a commitment not to increase a rate of duty beyond an agreed level) in

[7] See WTO, GATS, Article XVI.
[8] Ibid. Article XVII.
[9] Ibid, Article XVIII.
[10] See Mathew, note 6 supra,45-46
[11] Ibid.
[12] See http://www.wto.org last visited 5 May 2009.
[13] Ibid.
[14] See Amin Alhassan, 'Telecom regulation, the Postcolonial State, and Big Business: The Ghanaian Experience' *West Africa Review* (2003), http://www.westafricareview.comvol4.1.alhassan,html.
[15] See http://www.wto.org TELECOMMUNICATIONS SERVICES: LIST OF COMMITMENTS AND EXEMPTIONS Telecommunications commitments and exemptions
[16] Ibid.
[17] See http://www.wto.org last visited 10May 2009-05-12.

telecommunications is the objective of many of the negotiating requests made by WTO members to their trading partners. As of July 2008, 39 governments had made offers to improve their existing commitments or to commit for the first time in the telecommunications sector.

All in all, the trade rules that apply to telecommunications services include the framework articles of the GATS,[18] which contain the principles for trade in all services. In addition, the GATS also contains an Annex on Telecommunications. This provides guarantees for reasonable access to and use of public telecommunications, in a given market, by suppliers of all services benefiting from commitments scheduled by the member concerned. The Reference Paper (RP) is a set of regulatory principles that is legally binding for those WTO governments which have committed to it by appending the document, in whole or in part, to their schedules of commitments. There is therefore no telecoms regulatory regime that can dare ignore the contents of the RP document.

## 3. PRIVATIZATION AND THE LIBERALISATION IN AFRICA

As have been stated earlier, infrastructure industries have traditionally been monopolies, owned and operated by the public sector. Post-colonial Africa was no exception as it inherited *holus bolus* these models as for much of the 20th century, infrastructure services in all countries were provided by state-owned utilities that were vertically integrated.[19] In their initial stages these models produced some desirable results, later however, their service delivery ultimately led to serious problems for the public interest. The problems included underinvestment, in large part caused by under-pricing; low productivity; poor service quality; long queues and large portions of the population without access to basic services; lack of transparency; and damaging political interference in the operations of these infrastructure entities.

The primary aim of any liberalisation process is the achievement of effective competition. Black et al state that the theoretical justification for privatisation and deregulation comes partly from the potential efficiency gains to be had from a change in ownership and in market structure.[20] That in the telecommunications industry specifically, the justification comes also partly from a technological revolution which has effectively removed the need for state ownership and protection.[21] The other gains from privatisation stem from the sale of state assets which, coupled with the broadening of the tax base, may help governments to break out of their fiscal deadlocks and improve their ability to provide public goods and services to their respective constituencies.[22] Black et al further identify efficiency benefits which derive primarily from the nature of principal-agent relationships which are normally associated with a system of private ownership and competitive markets.[23] Under such a regime the principal shareholders will see to it that appropriate incentive schemes and monitoring procedures are put into place at all levels of management, thus 'minimising practices of moral hazard and adverse selection and setting conditions for maintaining high levels of operational …efficiency.'[24]

Black et al further argue that technological progress (or 'dynamic' efficiency) is likewise, likely to be more advanced under private ownership and competition than under a system of state control, since under the former system managers will more readily adopt new technologies aimed at cutting costs and boosting profits.[25] Quoting from previous issues of the *Economist*, Black et al state that with regard to the telecommunications industry, it is perhaps the technological revolution itself that has

[18] See WTO, GATS, Articles II-XV.
[19] See generally Calvin Djiofack-Zebaze & Alexander Keck, 'Telecommunication Services in Africa: The Impact of WTO Commitments and Unilateral Reform in Sector Performance and Economic Growth' Vol 37 No 5 (2009) *World Development*, 919-940.
[20] See P A Black, PO Baird & A Heese, 'Ownership and Competition in South African Telecommunications' Vol 65 (2) (1997) *South African Journal of Economics*,104-111.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.

triggered the world-wide restructuring and privatisation of the industry.[26] They opine that technological changes have affected virtually the whole of the industry, and are largely responsible for the introduction of optical fibres, digitised exchanges, mobile and cellular telephones, personal wireless handiphones, and electronic mail. They conclude that these changes have effectively broken down entry barriers and encouraged governments to liberalise and privatise the industry.[27]

Finally, Black et al state that whilst the process of privatization is still ongoing, it is generally necessary to impose price controls on dominant operators and, in a network industry, to allow new entrants, at least initially, to access the infrastructure of the incumbent.[28] This strategy was adopted by the South African government. The result was that a range of policy decisions on the part of the South African Government further entrenched Telkom's dominance and restricted the ability of competitors to access bottleneck facilities in a manner which would have enabled them to compete.[29] These included the restriction placed on value-added service (VANS) providers as to where they could obtain facilities. It has now been acknowledged that the unbundling of the local loop and opening international gateways (such as the SAT-3 undersea cable), to operators are pro-competitive interventions that have proven successful elsewhere. However when it comes to Telkom similar measures have not been imposed in South Africa.[30] Unfortunately, alongside a market structure wherein competition is inhibited, is ICASA, a regulatory authority which is equipped with such inadequate resources that will not enable it control Telkom's retail and access prices.[31] The general observation is that the South African telecommunications market is presently characterised by very limited competition and a regulator without the means necessary to control the dominant operator.[32] The result is that prices of telecommunications services are extremely high in relation to other jurisdictions. African governments have also given reasons for market access restrictions. Among others was the desire to give incumbents time to prepare for competition, for examples: Telkom in South Africa (fixed); Ethiopia (mobile & fixed); Cameroon (fixed). There was secondly the consideration to increase government revenue from privatization and the argument that exclusive rights were necessary to attract strategic investment, and to reserve exclusive rights in order to allow for the provision of universal service.

The challenge is for governments to develop capacity within their public service. Capacity building and training projects will enable governments analyse telecommunications market conditions; set policy frameworks; draw up, negotiate and enforce contracts; regulate monopolies; coordinate, finance and support producers; enable community self-provision; protect consumers and provide them with information on their options and remedies. There must however be realization that privatization is not the end of government participation but rather a new beginning. It is against this backdrop of complexities that this paper proposed the establishment of a regional telecommunications independent regulatory agency.

Many countries in Africa have completed the initial stages of reforming their telecommunication sector. Others are just initiating the process. All African countries seek to turn the digital divide into a digital opportunity and address the emerging broadband gap. Creating an enabling environment to attract investment is essential to meeting this goal. Policies being introduced deal with issues of

[26]See THE ECONOMIST (1993). "Selling the State", 21-27 August;THE ECONOMIST (1993). "Utilities & Telecoms: The Third Wire", 21-28 January;THE ECONOMIST (1993). "Asian Telecoms: Private Numbers", 30 September-6 October.
[27] Ibid.
[28] See Gershon Sibinda, 'Regulatory Environment Analysis in the South African telecommunications Industry' Vol 76(2) 2008 *South Africa Journal of Economics*, 213-227.
[29] See generally South African Telecommunications Sector Performance Review 2006, Steve Esselaar, Alison Gillwald & Christoph Stork (eds), LINK Centre Public Policy Research Paper No. 8 Learning Information Networking and Knowledge (LINK) Centre Graduate School of Public and Development Management Witwatersrand University.
[30] See ITU, CASE STUDY, BROADBAND THE CASE OF SOUTH AFRICA, 1-27.
[31] See Sibinda, note 28 supra, 225-227.
[32] Ibid.

privatization, establishment of national regulatory authorities, and enabling environment for competition. In 2007, Connect Africa reported that, at least, some thirty African economies (or 55 percent) had at least partially privatized their incumbent telecoms operator.[33] It has been observed that privatization sends a strong signal that policy decisions and regulations will be fair to all in the market place. The Connect Africa Background Paper opines that 'fostering a level playing-field is more likely if the State avoids being both a market player (i.e. owner or part-owner of the incumbent) and a referee at the same time."[34] In the same Paper, it is reported that forty-five African economies (or eighty-three per cent) have established a telecommunication/ICT regulatory authorities, with sixteen created since 2000.[35] However though in Africa some effective regulatory bodies have been identified, other continent's regulatory authorities lack the power to enforce pro-competitive regulatory decisions and many more require capacity building initiatives in order to become more effective regulators.

Rolling out fixed telephone lines is costly and few SADC countries can afford from their meagre resources such massive physical infrastructure. The capital is scarce, moreover savings are generally poor and the tax base very narrow. Foreign direct investment and policies related thereto should be specially addressed by a specialized body not an individual State communications department. As stated by Lydon and Williams, higher investment is central to achieving sustainable economic growth and poverty eradication.[36] Such higher investment can be achieved through FDI flows. In their study, Lydon and Williams, focused in particular on the relationship between FDI flows into developing countries and the penetration of telecommunications network in the recipient country. They found that both fixed and mobile communications networks 'are positively linked with inward FDI.'[37]FDI is also associated with privatization in the African market for mobile telephony.

## 4. MOBILE TELEPHONY AND PRIVATIZATION

Currently, mobile telephony is the most important mode of telecommunications in developing countries. It has been observed, that while internet access has become a reality for many businesses and public institutions, and for individuals with higher levels of education and income, for the vast majority of the low-income population, mobile telephony is likely to be the sole tool connecting them to the information society in the short to medium term.[38] Privatization has been brisk in Africa with regard to the liberalization of the mobile telephone industry.[39] Around 1996, telephone density in Africa was under one subscriber per 1000 inhabitants and it was thought that the region's development potential would be severely curtailed for a long time until this low density was reversed. However, by 2001, Africa reached a historic milestone with a density of one telephone subscriber per 100 inhabitants. The remarkable growth in so short a time has been attributed to the region's remarkable economic growth, the doubling of export trade, the liberalization of telecommunications, and the marriage between African subscribers to telecommunication services and mobile cellular and pre-paid card services. The underlying proposition is that, of all ICTs, mobile telephony has the most immediate potential to stimulate growth in the developing countries, and especially in Africa, in particular in sectors where entrepreneurship and access to market information are important factors. Mobile telephony has real economic consequences, particularly for micro-entrepreneurs.

The technology and infrastructure prerequisites saw **t**he majority of countries in Africa deploy GSM-based networks.[40] GPRS- and EDGEtechnologies have also been deployed in some of the comparatively developed mobile markets. Demand in broadband internet services is very high even

[33] See Connect Africa, 'Creating an Enabling Environment for Investment', Background Paper, Session 5 (20070 Connect Africa Summit, 20-30 October 2007.
[34] Ibid.
[35] Ibid.
[36] See Reamonn & Mark Williams, COMMUNICATIONS & STRATEGIES no 58, 2nd quarter 2005, 43.
[37] Ibid.
[38] See Information Economy Report 2007-2008, Chapter 8, 2.
[39] See generally, African Mobile Fact book www.africantelecomsnews.com last visited 3 May 2009.
[40] Ibid. 7-8.

though only few Africans are capable of affording them, making 3G service a viable business opportunity for mobile operators in the major cities in the continent. Some of the market players feel that 3G services will fill the void created in the regions where decent fixed line infrastructure is scarce and subscribers are unable to access the Internet.[41]

At least 15 mobile operators have already announced plans of introducing 3G services including existing networks in South Africa, Egypt and Tanzania and others planned in Kenya, Namibia and Nigeria. Only 5 percent of subscribers availed 3G voice and data service by 2006, according to Informa Telecoms and Media, an industry watcher. The relevance of mobile phones for small businesses in developing countries was noted in UNCTAD's *Information Economy Report 2005*. The use of mobile telephony in the conduct of business reduces the costs and increases the speed of transactions. Mobile connectivity sidesteps some important obstacles to other types of connectivity. It is not hampered by, among other things, cost and the remoteness of certain areas.

In Africa, mobile phones have proved so successful that in many cases they have replaced fixed lines. Almost 56 percent of the sub-Saharan Africa countries now allow competition in mobile cellular, up from 7 percent in 1995; only six countries lacked cellular services in 2001, compared with 28 in 1995; and 4 of 5 subscribers on the continent use pre-paid mobile service. Moreover, the growth in mobile cellular services is outstripping fixed telephone services by geometric proportions. In 2001, mobile cellular overtook fixed telephone subscribers for the first time, with 28 million compared to 22 million subscribers. By 2005, there will be 130 million phone subscribers in the region, 98 million of them mobile cellular subscribers.

There are several reasons for the rapid growth in mobile phone in Africa market. But the two most important are: first, the limited penetration of fixed-lines telephone network, lack of investment, inadequate private-sector involvement, foreign exchange scarcity (lack of trade), poor management incentives; second, the prepaid system which has its own advantages - low operating cost; no credit and less fraud than fixed line.

By 2007, the summary results of mobile telephony penetration in Africa was represented as follows:[42]

- At the end of 2007 there were over 280 million mobile phone subscribers in Africa, representing a penetration rate of 30.4 percent
- Africa has become the fastest growing mobile market in the world with mobile penetration in the region ranging from 30 percent to 100 percent from country to country.
- Fastest growing markets are in Nigeria, South Africa and Egypt
- Increased competition as more operators come online in each country (11 in Nigeria, 4 in Kenya and SA, 3 in Egypt and Morocco)
- Pre-paid subscriptions account for nearly 95 percent of total mobile subscriptions in the region.
- The Democratic Republic of Congo, population 60 million, has 10,000 fixed telephones but more than a million mobile phone subscribers.
- In Chad, the fifth-least developed country, mobile phone usage jumped from 10,000 to 200,000 in three years.
-

[41] Ibid.
[42] See **Mobile Penetration Statistics from Africa**, African Telecommunication / ICT Indicators 2008: At Crossroads.

## 5. COMPETITION AND FOREIGN CONTROL

There is fear that in future, the pioneer telecommunications service providers in the mobile telephony industry, may be vulnerable to international control, international sabotage, or to predatory economic practices. This in spite of the fact that the initial boon in mobile cellular telecommunications services in the continent was initiated by a new breed of pan-African mobile companies. These companies were in the first place not state-owned nor large multinationals as was previously speculated. This should be viewed against the background that, virtually in every country there is either lax regulation or weak regulatory framework for protecting both the new market providers and domestic consumers of cellular telecommunications services. The infant domestic telecom industry might not withstand the dominant multinational corporations economic power of competition. Multinationals in developed countries have huge advantages in technological and marketing capability, will enjoy comparative advantages over local industries. These multinationals will, once they enter the market, displace local operators and put them out of business as SADC telecom markets become attractive. The emergent players in the private telecommunications markets in the SADC region are not only small in market capitalization, but are failing to recognize the advantages of economies of scale. Players in these markets have not so far realized synergies by cooperating with one another. Instead, they are presently engaged in highly predatory and ruinous competition that leave them exposed and vulnerable to larger international entities who are making inroads into the SADC and Africa market. Eventually, the lucrative profits and revenues envisaged in the sector will in future accrue to foreign shareholders. Another observation made is that where strategic alliances are being made between providers of domestic mobile cellular services and foreign investors, the locus of control and strategic opportunities for both dominating and disrupting the markets of sub-Sahara Africa countries are located either in the United States, Holland, England, or the Middle East. And in some of these cases, the foreign partners have strategic alliances with military, industrial, and intelligence services in their host nations. For example, the major players, along with their home country affiliations in the African market include: RSA Security (Dutch/U.S.A.); MTN or Mobile Telephone Networks (South Africa); ECONET (Zimbabwe); PM Tech (U.S.A./UK); Oracle (U.S.A.); Microsoft (U.S.A.); and Orascom (Egypt).

The density of integration of the African communications networks with the foreign operations is as remarkable as it is invisible to all but the most critical observers. First, there is the element of platform interconnectivity, as in the joining of the West African Submarine Cable (WASC) system with the South African Far East (SAFE) cable system.[43] SAFE is submarine fibre optic cable measuring 28,000 kilometres and linking Europe to Africa and Asia, designed to carry telephone, multimedia and internet traffic. This huge project, costing USD640 million, was financed by a consortium of 36 international operators including France Telecom, which invested USD96 million or 15 percent of the total. The SAT-3/WASC/Safe submarine cable will enable broadband telecommunication services in particular to be strengthened.[44] Also, the West Africa Cable System (WACS) will boost broadband capacity and could cut comparatively high Internet tariffs in Africa's biggest economy, which has relied on a single international cable controlled for years by Telkom.

What is curious about this SAFE system is that it is anchored in Kochi, Kerala (India). But its operations and the profile of the services it provides have significant implications for Africa and many non-African countries. West Africa is also currently served by two cables (Atlantis II and SAT-3).

[43] See further http//wwwglobalinsight.com, where it is stated that Portugal Telecom and its subsidiary Cape Verde Telecom have reportedly invested US$50 million in a West African submarine cable WASC), which will connect Cape Verde and Portugal. According to *Macau Hub*, the investment is part of an international consortium. The report says that the cable will run along the west coast of Africa and have landing points in Cape Verde, Portugal, and London; it is due to become operational in 2011. Besides Cape Verde Telecom, in which Portugal Telecom owns a 40% stake, the operator also has subsidiaries in Morocco, Guinea Bissau, Sao Tome & Principe, Angola and Namibia. According to *Macau Hub*, Portugal Telecom plans to use the cable for connectivity to some of its African operations as well as its own Internet connectivity to the hub in London. Cape Verde Telecom had an international bandwidth of 24 Mbps in 2006 and 68 Mbps in 2007

[44] See SAFE http://www.safe-sat3.co,.za

Besides, seven more are planned; namely, Glo-1, Main-1, WAFS, Infinity, Uhurunet, AWCC/WACS, ACE. The investment would either be into the WACS cable which would run to London, or more likely the ACE (Africa Coast to Europe) cable planned by France Telecom which would run via Cape Verde and Portugal to France.[45]

With this type of integration, cable and satellite services have been linked between Far East Asia, Africa, and Europe, with connection points in India, Durban, the Reunion Island, Mauritius, Malaysia, Melkbosstrand (S. Africa), Angola, Gabon, Cameroon, Nigeria, Benin, Ghana, Senegal, the Canary Islands, Spain, and Portugal. The system, with its controls in India, already has 42 telecommunications companies located in 35 countries using its services.

Platform interconnectivity via computer and database-linked systems such as those provided by the U.S.-based Microsoft and the Oracle corporations, illustrates, the now dominance of foreign telecom operating entities in Africa. Although they provide no visible mobile cellular telecommunications services, they control and virtually own the hardware operating systems platforms, the routing networks, the databases, and the appliances that run and remotely monitor every computer and database operation in the region. Of late, Microsoft, has struck strategic partnership with PM Tech Holdings for software solutions development, networking, database management, e-security, and IT (information technology) consulting.[46] PM Tech already has extensive holdings in the petroleum, financial, telecommunications sectors of Nigeria, Cameroon, the Congo, Swaziland, Botswana, and it is rapidly expanding its operations throughout West Africa. Also, it is targeting Kenya, Namibia, Mozambique, and Zambia. Oracle Corporation has already set up shop in Abidjan as a regional hub and with its business applications suites and networking solutions already controls 80 percent of all public administration projects in West Africa, all banking operations, telecommunications services, and is seeking to establish strategic partnerships with companies with defense industry links.[47] RSA Security, a major South-African military defense industry subsidiary at one point, has Dutch and US affiliations with headquarters in Bedford, MA.[48] The company's expertise includes electronic security solutions and e-security intelligence and it has established strategic partnership with Schlumberger-Sema, a global information technology services company, to provide smart card-based solutions that interface with RSA Security smart cards operations in banking and other services throughout Africa. RSA Security already boasts 12 million customers worldwide. In 2001, e-security solutions accounted for 100% of RSA Security revenues. In 2000, the company reported a gross income of $280.2 million and an after-tax profit of $205.8 million. Econet, a small Zimbabwe wireless company, secured in 2002 contracts worth $50 million to deliver international commercial satellite services to customers, providing linkage between African countries and Europe, allowing Econet to gain European footprints, but with heavy reliance and dependence on UK companies that provide the gateway into Europe. Then, as a last there is Orascom as a last example. Orascom is an Egyptian company, with 57 percent of the stock held by the Sawaris family of Egypt, presently operating in 18 Middle Eastern and sub-Saharan Africa countries, with a mobile cellular link hub in Belgium.[49] Orascom's core business activities are extensive and touch on a wide swath of sub-Sahara Africa life -- IT, computer-related services, hotels, medical, dental, hospital supplies, construction and petroleum services.

These inroads by foreign capital, now translating into multibillions of US dollars, will eventually swallow infant industry in the SADC region in the whole of the telecommunications sector. Weak, economically underdeveloped, sometimes corrupt States in the SADC region might never have power to coordinate and monitor the dangerous and negative activities of these companies in a sector industry which is by its nature, capital and resource intensive, and deploying highly skilled personnel in all its

[45] Ibid.
[46] See www.pmtech.net last visited 12 May 2009.05.12
[47] See Oracle The World's Largest Enterprise Software Company http:www.oracle.com/index.html last visited 11 May 2009.05.12
[48] See RSA SecurityD http://www.rsa.com/mode.aspx?id+1156 last visited 10 May 2009.
[49] See http://www.otelecom.com/ last visited 9 May 2009

divisions.

## 6. SADC COMMUNICATIONS INDEPENDENT REGULATORY AUTHORITY

The Southern African Development Community (SADC) has been in existence since 1980, when it was formed as a loose alliance of nine majority-ruled States in Southern Africa known as the Southern African Development Coordination Conference (SADCC), with the main aim of coordinating development projects in order to lessen economic dependence on the then apartheid South Africa. The founding Member States are: Angola, Botswana, Lesotho, Malawi, Mozambique, Swaziland, United Republic of Tanzania, Zambia and Zimbabwe. The present States membership include: Angola, Botswana, the Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, United Republic of Tanzania, Zambia and Zimbabwe.

The need for the establishment of an independent regulatory authority for telecommunications in the SADC region is motivated by the existence of a number of factors political, economical, developmental, and all in the ever globalizing world. One of the central objectives of SADC is to forge links among Member States to create a genuine and equitable regional integration and promote advancement of its citizens, thereby raising the quality and standard of life and, consequently, alleviating poverty. The enabling factors to achieve this goal include: co-operation in infrastructure development, coordination of sectoral plans and programmes, promotion of investment and production, and the development of indigenous contents, are still being harnessed.

The telecommunications has been identified by SADC members as one of the key infrastructures that still has to progress to the desirable standard. A large scale and advanced telecommunications infrastructure in SADC, capable of delivering telecommunication services, has been recognised as a pre-requisite for economic growth. Therefore, the availability of adequate communications links within both individual countries, the region and internationally is accepted by stakeholders as an essential instrument to facilitate intra-SADC and extra-SADC trade, leading to socio-economic development. It has however been acknowledged in the region and confirmed through various studies, including those of the International Telecommunications Union (ITU), that there is a serious inadequacy of info-communications capacity.

As the free movement of goods, services, labour and capital intensifies, the telecommunications sector is certainly going to be capitalized in massive proportions and become complex to regulate. In place must the therefore be an independent, efficient, effective, transparent, well-funded and well staffed, technologically endowed regional regulatory regime. A regime capable of engaging and reining the power and economic dominance of multination companies and other powerful stakeholders in the ICT sector, in particular the Telkom corporate group structure.

There are a variety of explanations for the adoption of regulatory statutes or treaties, most of which amount to justification. Regulatory legal regimes can be distinguished according to function. Sunstein asserts that many statutes in this regard are responding to market failures.[50] For example, in the field of regulation against a monopolistic business practice, regulatory statutes are, least controversially, a response to the risks of monopoly. Regulation may be a response to collective action problems, coordination questions and transaction costs.[51] Sunstein states that it is a familiar point that individually rational private behaviour may produce collective or public irrationality.[52] For instance, if everyone acts in his/her self-interest, serious harm will sometimes result. Instances in this regard involve public or collective goods which are characterised by two features, non-rivalrous

[50] See Cass R Sunstein 'The Functions of Regulatory Statutes' in G Teubner (ed), *After the Rights regulation: Reconceiving the Regulatory State* (1990), 48-55; see also Barry Barton 'The Theoretical Context of Regulation' in Barry Barton, Lila K Barrera-Hernández, Alastair R Lucas & Annita Ronne (eds), *Regulating Energy and Natural Resources* (2006)), 16-17.
[51] Sunstein, note 50 supra, 49.
[52] Ibid.

consumption and non-excludability. In cases of this nature, each person acting rationally is tempted to 'free ride' while others pay, the consequence being that the good would not be provided for all. Sunstein states further that government regulation is needed to eliminate the free-rider problem and to ensure the public goods will be created.[53] However in this paper I deal with a regulatory agency of a special kind, an independent regulatory agency (IRA), on telecommunications dealing with ICT services and goods and personnel with an ICT infrastructure. A regime that owes its creation to a collective group of independent who have undertaken to shed part of their sovereigny to establish a regulatory regime that is not accountable to any particula State. The strategy is to avopid capture by any State member or a particular State Ministry. Opportunities for corruption are immediately eliminated in a sector valued in trillions of US dollars, and still growing in tandem with the nergy sector (not discussed here).

Accordingly, in this paper, an IRA is exclusively defined as an agency having its own powers and responsibilities under public law; whose organizational structure is separated from government ministries and whose members are neither directly elected by people nor managed by elected officials. If these are the minimum requirements that this regional IRA should meet in order to be counted as really independent, then those agencies which are organized as units of ministries, organic organs of government or within the bureaucracy should be excluded from the analysis, because these latter referred to formations are exercising state power under the direct control of ministers and the civil service. Moreover, their powers and institutional designs are not independent from the government. Immediately therefor Telkom (SA) and other State utilities in the telecommunications sector are excluded from participating in this envisioned regional IRA, and this includes ICASA.

This envisaged regional IRA structure will also have intergovernmental features, though not monopolised by a single parliament (or ministries) of participating States in that there will be regular consultative summit with State Ministers in charge of ICT and infrastructure. It must be understood that ICT products are cross-cutting, multi-media and defy geographical boundaries. Added to these factors are the magnitude, technical complexity and the variability of the material or entities being regulated. There is also a need to remove these matters from direct political control and to follow a quasi-judicial mode of procedure that includes enforcement. As stated by Barry Barton,[54] regulation (independent regulatory authority) often pursues multiple processes and is also a matter that cannot be left to the courts of law. Barton also distinguishes the relative roles these two institutions (courts and regulatory agencies) play. He states that,[55]

> regulatory agencies must often develop and implement policy consistently with other public agencies, while the courts are independent. Regulation is generally a long-term engagement with an area activity, while the judicial process is one of deciding each matter that is brought to court. Regulation usually looks ahead, while the courts are usually concerned with applying the law to past events. The focus of regulation is the management of an area of activity, as applied by law, rather that the determination of rights under the law…

Barton also offers a cogent argument why on the other hand regulation is not left in the hands of the executive. He states,

> [i]n the United States in particular, regulatory agencies were established because it was necessary to entrust aspects of the public interest to independent scientific experts, removed from politics, and from outside the normal civil service framework.'[56]

A number of initiatives have been undertaken by several institutions, including the ITU to address this critical problem. One valuable initiative is the African Green Paper that focuses entirely on the

[53] Sunstein, note 50 supra, 49.
[54] See Barry Barton 'The Theoretical Context of Regulation' in Barton et al, note 50 supra,15.
[55] Ibid.
[56] Ibid.

problems of telecommunications in Africa and offers a comprehensive policy guideline for countries in Africa to harmonise telecommunications sector policies as a strategy to develop telecommunications infrastructure and services. There is also the SADC Protocol on Transport, Communications and Meteorology which prescribes the development of a harmonised regional policy with the provision of reliable, effective and affordable telecommunications services, as its central goal. The Protocol specifies actions that will have to be undertaken to transform the state of the national and regional telecommunications infrastructures from their present state of under-capacity to an integrated and advanced info-communications network.

Regional policy on telecommunications becomes even more crucial in this period of globalisation of the world economy, where telecommunications is reckoned as both a tradable service and transport of info-communications services. In this context, the capability of an individual State for effective delivery of services is not likely to contribute to stronger regional co-operation. Instead there is now unnecessary duplication of structures and efforts, dissipation of funds from foreign donors directed to improve individual State's ICT structures but diverted to other irrelevant programmes or projects through capture and failure to prioritise. From the beginning two benefits may be realised.. Firstly, a group of countries combines their strengths, on one hand, to resist competitive threats and, on the other hand, to take advantage of the opportunities that emerge in the global market, such as the transport of international telecommunications or information traffic. Secondly, the group of SADC countries will present a larger market to private investors who could find an opportunity to achieve standardisation and economies of scale, factors that may be decisive in investment decisions. Finally, the interest of society as a whole must be taken into consideration in any decision affecting the development of the telecommunications industry.

## 7. RECOMMENDATIONS

A. Establishment, through treaty and protocols of the SADC Independent Communications Authority (SADC-CA).

B. The personnel should be independent of and not be appointees of SADC member States governments; neither should the personnel be drawn from SADC related ministries.

C. SADC-CA will hold quarterly consultative summit meetings with SADC telecommunications ministries and other relevant bodies, with a major mandate to develop and adopt Telecommunications Acts and other ICT related rules and regulations.

D. All the functions of the already existing telecommunications agencies under State ministries, and those of existing so-called independent regulatory agencies would be subsumed under SADC-CA.

E. Funding of SADC-CA will come from contributions made by SADC member States – from each according to its means in terms of a certain percentage of a State's GDP. Consequently all the employees of SADC are paid from the fund administered exclusively by the Authority.

F. Foreign ICT aid presently enjoyed by respective individual States, will in future be directed to the exclusive use of the Authority – to minimise abuse by political leaders and to avoid stakeholder capture.

## 8. CONCLUSION

The world is witnessing an upsurge in the use of telecommunications and information in nearly all aspects of human endeavour. The wireless revolution and the internet phenomenon have recently changed the way people live and transact business, and the telecommunications/information technology industry has taken centre stage in world affairs and will continue to be so far into the foreseeable future. The WTO has confirmed that the world telecommunications and information technology industry was worth US$ One trillion in market capitalization. In Africa, there is however

dearth of telecommunications infrastructure, though the penetration has been noticeable over the past decade, mostly through the dismantling of State monopolies, especially the telecommunications State utilities, sustained without an efficient telecommunications infrastructure. Telecommunications and information technology present copious opportunities for the creation of unprecedented wealth for Africa. For Africa to benefit from these opportunities, it needs to improve services by eradicating misuse of monopoly powers and inefficient use of public resources, The African States need also remove policies that fostered and encouraged the dominance of the public sector in national economies in order to attract modern industries and business - of course to attract foreign investment. Granted some significant progress has been made in some countries, though there are challenges on the way. There is now a general awareness all over the continent of the need for liberalisation, with some countries moving faster than the others. Some countries have embraced liberalisation and there have been remarkable progress, thus encouraging others to move in the same direction. Studies associate foreign direct investment with economic growth rates, and that improvements in the telecommunications industry stimulate FDI inflows. The framework for these reforms is provided for by GATS in terms of its overall annexures. The telecommunications industry is complex and resource intensive and requires massive capital outlays. The industry also demands highly skilled and technologically endowed personnel. Such skills and capital are not readily available in Africa. In the SADC region the level of savings is very low and the dominance of the South African economy and its multinationals is a cause for fear. The SA'S State's utility, TELKOM, is still under managed liberalisation. It would be in the interest of the SADC region to establish through treaties and protocols a regional independent communications regulatory authority. This will require that SADC member States relinquish part of their sovereignty and allow their respective regulatory agencies to be subsumed under the envisaged independent regional regulatory agency (IRA). This regional IRA will have powers to deal with excesses designed by multinationals while levelling the playing field, giving certainty to the markets whilst providing security to investors. The WTO Reference Paper which is a blueprint for the telecommunications sector can always be consulted by policy makers when developing future policies, rules and regulations for an acceptable efficient, effective, transparent regulatory regime. Highly skilled personnel should be recruited and trained. To avoid capture by dominant stakeholders all the personnel regulatory agency will not be accountable to their respective home governments. The regulatory regime will be in charge of its own funding and finances and will regularly hold quarterly consultative summit meetings with ministries relevant to the telecommunications industry.

# Is South Africa's ICT Regulatory Framework Still a Barrier to Entry?

**Carmen Cupido**
Bowman Gilfillan
Johannesburg, South Africa
c.cupido@bowman.co.za

**ABSTRACT**

With the August 2008 court ruling against the Independent Communications Authority of South Africa (ICASA) and the Minister of Communications with respect to the right of Altech Autopage and about 550 similarly situated parties to receive individual electronic communications network service and electronic communications service licences, [1] the South African telecommunications sector overnight was significantly liberalized on a par with some of the most liberalized telecommunications environments in the world. But, the prices we pay for communicating remain among the highest in the world. Is this because we are still waiting for the much-lauded submarine cables to bring us capacity? Or is it because our regulatory framework still prefers a few big players over a multitude of smaller service providers and regulates to this effect? This paper will set out why I think the correct answer is the latter.

This paper deals first with the two aspects of the regulatory framework in the telecommunications (as it was known then) industry that has always been regarded as the highest barrier to entry namely licence fees and the cost and allocation policy with respect to spectrum or frequency.

Then, I will discuss the implications of the Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act (Amendment Act), published on 9 January 2009, which has, as from 1 July 2009, amended the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (the Act). [2] The Amendment Act provides anew for information to be obtained and kept in respect of cellular phones and SIM cards and extends the application of these provisions of the primary Act. It also provides for expanded penalties and offences.

In the next section I outline certain salient aspects of the regulatory framework in South Africa, including the e-rate, expanded consumer protection and universal service obligations, within which new entrants (and incumbents) operate in the electronic communications services sector and present an outlook as to the implications for increased and more efficient competition in the ICT and related industries.

## LICENCE FEES

On 1 April 2009, ICASA published the General Licence Fee Regulations [3] prescribing the administrative fees payable in respect of an application or registration of a licence, amendment, transfer or renewal and the annual licence fees payable by licensees in terms of the ECA. The regulations provide for the exemption of the following classes of licensees from the payment of annual

[1] *Altech Autopage Cellular (Pty) Ltd v Chairperson, Council of the Independent Communications Authority of South Africa*, case no. 20002/08, North Gauteng High Court (unreported).

[2] Proclamation 39 in *Government Gazette* 32341 of 22 June 2009. Section 3 of the Amendment Act will come into effect on 1 August 2009.

[3] GN 345, *Government Gazette* 32084 of 1 April 2009.

licence fees –

- class licences for community Broadcasting – sound and television;
- individual licences for public broadcasting services – the SABC; and
- Licensees who satisfies the turnover threshold to be classified as a small enterprise.

Annual licence fees are set at 1.5% of Gross Profit (total revenue derived from licensed services less total costs directly incurred in the provision of such services). The calculation of the amount due must be based on audited financial statements (or sworn statements where audited statements are not required by law), which must be submitted along with the payment. Fees can be paid quarterly or annually and the deadline for final payment in respect of any financial year is six months from the financial year end of a licensee. Late payments will be subject to stiff interest penalties and fines for non-compliance. Licensees with an annual turnover of less than R13 million are exempted from the obligation to pay annual licence fees (but will still need to file something analogous to a zero return).

The regulations are vague as to the manner in which licence fees are to be calculated in practice. For instance, there is no definition of Gross Revenue (GR) nor any guidance on what will be regarded as Total Costs (directly incurred in the provision of licensed services). In the absence of any specified method for calculating Gross Revenue (GR) for the purposes of the calculation of Annual Licence Fees payable, licensees would be entitled to undertake this calculation in any reasonably justifiable and appropriate manner. There is, further, questions over the interpretation over the meaning of the term "licensed services".

Except for the vague drafting, the major issue with the regulations relate to the need to shift the Telecommunications Act mindset which still pervades ICASA. This means that although ECA was enacted to level the playing fields, so to speak, by "flattening' the licensing structure. And some of that thinking has filtered down to the courts, handing down various decisions in support of a more equal market structure. These regulations are counter-productive in the sense that it applies the same level of regulation to geographically lesser players with class licences as it does to the ones with international connectivity, regional networks and billions in revenue. For instance, the class licences were supposed to be a category of licences that would attract minimum regulation, but ICASA has slapped it with a hefty registration fee of R10 000 and annual licence fees of 1.5% of GP, the same as individual licence holders. This may not seem excessive to the bigger players in the market, but this fact coupled other regulatory taxes can put the squeeze on the smaller players. ICASA should, in this regard, consider a tiered approach that will ease their administrative burden at the same time.

## SPECTRUM FEES

This issue will be discussed with reference to the much-contested 2.6 and 3.5 GHz frequency bands, the so-called Wi-MAX bands. The allocation of these frequencies has been the subject of numerous discussion documents calling for input and public hearings, culminating in ICASA publishing on 17 June 2008 a decision document [4] outlining its position on how to allocate spectrum where demand exceeds supply as is the case with the frequency bands under discussion. The major issue around spectrum regulation and allocation is that it is a scarce national resource the regulation of which must be in the national and public interest and must conform to international instruments and precedent.

In light of the finite nature of the resource; it is important that it is optimally used and to that end the ECA provides for ICASA to withdraw any radio frequency spectrum licence when the licensee fails to utilize the allocated radio frequency – the so-called "use it or lose it" provision. ICASA is required to

[4] GN. 748 in *Government Gazette* 31150 of 17 June 2008.

make regulations to give effect to the legislation. As it stands, however, the incumbents hold the following blocks of spectrum in the 3400 – 3600 MHz (3.5 GHz) band -

- 2 x 28 MHz to Telkom;
- 2 x 28 MHz to Neotel; and
- 2 x 14 MHz to Sentech, within the 3.5 GHz band; leaving a total of 60MHz available for further assignment.

In the 2.6GHz band Sentech has an assignment of 50MHz and Wireless Business Solutions (WBS) has 14MHz which leaves 126 MHZ unassigned.

Information on whether the current assignments are being used efficiently or at all is not available. This appears to be a case of "spectrum hoarding" by incumbent operators to stifle competition, with the acquiescence of the regulator. The decision document, referred to earlier, states that 80% of the 3.5GHZ band has been permanently assigned. I submit that the "permanent assignment" of spectrum is contrary to the spirit of the ECA which provides for regulation in the public interest and in contravention of actual provisions of the ECA which provides for spectrum licensing and licensing conditions to be adhered to, specifically the legislative provision of "use it or lose it" as it relates to frequency spectrum.

In the decision document on WiMax spectrum licensing, ICASA states that it will allocate the remainder of the 2.6 GHz spectrum that has not yet been allocated, to six national licensees in 20MHz blocks, on a technology-neutral basis and the remainder of the 3.5 GHz spectrum to two regional operators per local municipal area with 2x15 MHz spectrum each. This allocation will be preceded by a two-step qualification process i.e. a beauty contest followed by an auction. ICASA states in this regard that the most important issues to be decided in the pre-qualification beauty contest phase is the extent of inclusion of historically disadvantaged individuals (HDIs) in the following areas –

- Minimum 51% black owned, with an emphasis on women, in line with the Broad-based Black Economic Empowerment Act 53 of 2003;
- Levels of participation by HDIs in the management and control of enterprises in line with Employment Equity Act 55 of 1998;
- Affirmative procurement in line with Preferential Procurement Policy Framework Act 5 of 2000;
- Commitment to skills development of HDIs in line with the Skills Development Act 97 of 1998.

With respect to the allocation of the rest of the frequency spectrum, there has been no real progress in assigning frequency to new entrants although ICASA has issued for comment draft regulations intended to update the manner in which fees for the use of licensed radio frequency spectrum are calculated. The Draft Radio Frequency Spectrum Fees Regulations 2009 and the Draft Radio Frequency Spectrum Fee Discussion Document proposes the adoption of Administrative Incentive Pricing (AIP), which is a methodology proven to assist in increasing the efficiency with which spectrum is used. The regulations are based for the most part on similar regulations enacted by OFCOM – the electronic communications regulator in the United Kingdom. [5]

## REGULATION OF INTERCEPTION AND MONITORING OF COMMUNICATIONS

Much of the controversy surrounding legislation designed to provide law enforcement authorities with

[5] Opinion prepared by Dominic Cull, accessed on 20 June 2009 at www.ellipsis.co.za

a framework to legally intercept and monitor communications has not been removed by the new Amendment Act.

The Act, which places onerous obligations, financial and otherwise, on service providers in the electronic communications industry, is applicable to direct (one-to-one) and indirect (electronic) communications, both in the workplace and the private sphere.

Fortunately, the default position under the Act is that all monitoring and interception of communications is prohibited unless it is provided for and authorized in terms of the Act or carried out by law enforcement officials in terms of an interception direction issued by a judge.

The original Act, prior to its amendment by the Amendment Act, provided that certain information was required to be obtained and retained by mobile cellular operators in respect of their customers. The coming into effect of these provisions of the Act was delayed since 2005, when the rest of the Act came into operation, because of lobbying by the mobile cellular operators, who highlighted numerous practical difficulties around the implementation of the provisions in question. Through the introduction of new sections 40, 62(6), 62A, 62B and 62C, the Amendment Act has now altered these provisions of the Act, introduced new definitions into the Act and provided for strengthened penalties for non-compliance.

## SECTION 40

This section's heading is "Information to be obtained and kept by electronic communication service provider who provides a mobile cellular electronic communications service". Section 40 of the Act came into effect on 1 July 2009, being the date on which the Amendment Act came into force.

Aptly named, section 40 of the Act precludes a SIM card from being activated unless the service provider, at its own cost, recorded and stored, in case of South African citizens, the customer's full names and surname, one address (if a permanent South African resident) and his or her identity number.

For foreigners and non-residents, the full names, identity number, at least one address and the country where his or her passport was issued, must be recorded and stored.

While these requirements are not especially problematic in relation to post-paid contract subscribers, who generally already provide the requisite information to their service providers, the Act has significant implications for service providers in relation to their pre-paid subscribers who have not previously had to provide any such information. This section also obviously has implications for tourists having to comply with these provisions before being allowed to purchase and use a pre-paid SIM card from a local operator.

If a juristic person – like a company or trust – wishes to buy and activate a SIM card, the personal information of the juristic person's authorised representative and, where applicable, the registration number of the entity are required to be provided.

Sections 40(3) and (4) of the Act require the service provider to verify the information recorded and ensure that the processes and systems for recording and storing the information are secure and accessible only to authorised persons, to prevent the misuse of information collected in this manner.

Section 40(5) obliges any person who "sells or in any manner provides an activated SIM card to a[nother] person, other than a family member", along with the person who is to receive the SIM card, to furnish their full details to the service provider, who must verify the information (section 40(6)).

In terms of section 40(8), if a staff member of a service provider suspects that an identity document furnished to activate a SIM card is false, the suspicion must be reported to a police station within 24 hours.

An applicant may, when applying for an interception direction to intercept or monitor electronic communications, request a service provider to confirm whether a particular person is a customer and provide the personal information in relation to that person which has been recorded and stored (section 40(7)).

In addition to the personal information in relation to a service provider's customers which is required to be recorded and stored, section 40(9) of the Act obliges every service provider also to store the number pairs (MSISDN and IMEI) [6] associated with every mobile terminal.

In terms of section 40(10), all the information which is required to be obtained and kept by a service provider must be stored for five years after the customer or the service provider terminated the contract for the provision of mobile services.

**SECTION 51**

The Amendment Act provides for the amendment of the offences and penalties provisions of the Act and imposes significant penalties for non-compliance with the requirements discussed previously. These will come into effect on 1 August 2009.

Once these provisions have come into effect, in terms of section 51 of the Act, contravention or failure to comply with obligation to obtain and store the personal information of its subscribers and other information in relation to the SIM cards and handsets sold, will an offence to which a service provider will, upon conviction, be liable to a fine not exceeding R100 000 for each day that failure to comply continues.

The failure by a customer of a service provider to comply with the obligation contained in section 40(5) to obtain personal information from any person to whom that customers sells a SIM card and to pass that information on to the service provider and by an employee or agent of a service provider to comply with the requirements of section 40(8) to report any suspicious identification document is an offence and, upon conviction of which, the customer, employee or agent, as the case may be, is liable to a fine or imprisonment not exceeding twelve months.

**SECTION 62**

The transitional provisions of the Act, which are contained in section 62 of the Act, provide for the phasing-in of the information recording requirements described previously in relation to the existing customers of a service provider of mobile cellular services. In terms of section 62(6) of the Act, a service provider who furnished a mobile cellular communications service before the commencement of that section of the Amendment Act (i.e. 1 July 2009) is obliged to record and store its existing customers' information in terms of section 40(2) of the Act. This must be done within eighteen months i.e. by 1 January 2011). Although this information would previously have been provided to service providers in respect of their contract subscribers, it would not generally have been provided by pre-paid customers. Where the required information has not been recorded and stored within this time period, the mobile services utilizing any activated SIM card must be discontinued.

The effect of these provisions is that pre-paid customers could be cut off unintentionally if they do not furnish their service providers with the relevant information. The steps which will need to be taken by

[6] Mobile Station Integrated Services Digital Network (MSISDN) is a Mobile Station ISDN number. ISDN is a set of international standards set by the International Telecommunication Union – Telecommunications (ITU-T) for a circuit-switched digital network that supports access to any type of service over a single integrated loop from the customer's premises to the network edge; see *Newton's Telecoms Dictionary*, 24th edition.

International Mobile station Equipment Identity (IMEI) is an equipment identification number, similar to a serial number, used to uniquely identify a mobile phone.

the various service providers to facilitate compliance with these obligations are a significant administrative burden. This has the potential to increase the cost of doing business in the South African ICT sector and to upset customers whose services are cut off. Although some compensation is payable to mobile operators for the actions they are required to perform to facilitate the interception or monitoring of communications by law enforcement officials, [7] no compensation is payable to such operators and other service providers selling those operators' mobile services in complying with the obligation to obtain and store their customers' personal information and information in relation to SIM cards and mobile handsets.

## E-RATE

Amongst the other obligations which are imposed on providers of communications services in South Africa is the requirement to levy a reduced rate, known as the e-rate, for the provision of Internet services to certain educational institutions. In terms of section 73 of the Electronic Communications Act 36 of 2005 (ECA), Internet services must be provided to all public schools and all public further education and training institutions at a minimum discounted rate of 50% off the total charge levied by the entity licensed to provide such services.

ICASA published on 3 March 2009, regulations with regard to the implementation of the e-rate. [8]

These regulations provide that all electronic communications services (ECS) and electronic communications network service (ECNS) licensees must offer Internet connectivity to public schools, public tertiary institutions and certain designated private educational institutions at 50% below the total charge levied by the licensee for the provision of such services. Failure to comply with this requirement could give rise to a maximum penalty of R150 000.

This is not insignificant considering that the regulations are unclear in various respects. First, the regulations do not specify which price must be discounted by 50%. There are some indications that ICASA intended that the fee charged by licensees to educational institutions for the provision of Internet services should be the lowest commercial rate charged to other customers by the licensee in question, which would then be subject to the 50% e-rate discount. However, although the regulations define 'retail rate' as the lowest commercial rate charged for a service, but this term is not used in the regulations. Regulation 3 then provides only that licensees must discount their "total charge levied" by 50%. The manner in which the regulations are presently drafted has the effect that operators are able to grant a discount on their highest rather than their lowest retail prices, thus potentially negating the benefit that the e-rate was intended to confer on educational institutions. This clearly seems to be contrary to the intended effect of the e-rate provisions of the ECA.

Successful implementation of the e-rate may further be hampered by the definition of "internet" in the regulations and the provision that the e-rate discount is applicable to, amongst other things, "connectivity charges for access to the internet". "Internet" is defined as "a collection of interconnected computer networks using the Internet Protocol (IP) allowing them to function as a single large virtual network." It seems clear that the e-rate discount is intended to be applicable to all Internet services provided to schools, which would include as voice over IP, IP television and video streaming. Such services are relatively data heavy services. It is conceivable that Internet Service Providers may refuse to provide services to schools because of the requirement that all Internet services, rather than only basic Internet services are required to be provided at the discounted rate which may have an impact on the viability of their business cases.

[7] Notice in terms of section 31: Mobile Cellular Operators published in GN R93 in *Government Gazette* 31844 of 6 February 2009.

[8] GN R246 in *Government Gazette* 31979 of 3 March 2009.

## CONSUMER PROTECTION AND UNIVERSAL SERVICE OBLIGATIONS

ICASA has published the following regulations in respect of consumer protection –

- Code of Conduct for electronic communications service (ecs) and electronic communications network service (ecns) licensees[9] ("the Code of Conduct")
- Regulations setting out minimum standards for end-user and subscriber service charters[10] - under review; and
- Code in respect of people with disabilities applicable to all licensees[11]

The Code of Conduct is applicable to ecs and ecns licensees and must form the basis of individual codes to be developed by licensees for their own businesses and it must be applied in accordance with relevant legislation. The Code of Conduct further sets out the general standards to be adhered to by licensees with respect to consumer rights, contract terms and conditions and consumer confidentiality and charging, billing, collection and credit practices.

The regulations setting out the minimum standards for subscriber and end-user service charters are currently under review by ICASA. The regulation provides, amongst others for the optimum availability and reliability of service – 99.9% of actual area of coverage. The average time to install and activate a service must be fourteen days and call failure rate must not exceed two percent. Further, operator response time may not exceed 3 minutes for all operator assisted calls, directory enquiry services, call centres and other non-emergency services. In addition the licensee, at its own cost, must maintain an Electronic Communications Network Monitoring Centre, operating twenty-fours a day, seven days a week.

The regulations setting out protection for disabled consumers prescribes basic standards for accessibility and availability in respect of text telephones, public access devices and community service telephones; and that operator assistance and other services at call centres, telephone bills, contracts, advertisement and promotions must be offered in appropriate formats, making it accessible to disabled consumers.

Licensees must report on the progress of implementation of the above measures to make services more accessible to disabled persons.

## UNIVERSAL SERVICE OBLIGATIONS

The regulations[12] in respect of the prescribed annual contributions of licensees to the Universal Service and Access Fund (USAF) provide that licensees (class and individual) must pay an "annual contribution of 0.2% of the annual turnover, derived from the licensee's licence [sic] activity to the Fund". Included are also private ecn reselling excess capacity and broadcasting licensees who may setoff their contribution to the Media Development and Diversity Fund against the prescribed contribution to the USAF.

As in the case of the licence fees, hefty penalties and interest payments are levied against late payments.

---

[9] GN R1740 in *Government Gazette* 30553 of 7 December 2007.

[10] GN R1166 in *Government Gazette* 31556 of 31 October 2008.

[11] GN R1613 in *Government Gazette* 30441 of 7 November 2007.

[12] GN R1270 in *Government Gazette* 31499 of 10 October 2008.

## CONCLUSION

The question that was asked in the introduction was whether regulation is the issue that keeps our prices high.

By only looking at the extra costs that must be incurred by operators in our industry, i.e. licence and spectrum fees, RICA Act compliance, the e-rate, consumer issues and universal service obligations one can't help but think that regulation is definitely a factor, and not an insignificant cost factor – "directly incurred in the provision of licensed services". The cost of regulation is, however, not the only fact, there are others that are directly related to regulation (or the lack thereof) that keep prices high such as the interconnection regime.

So, in conclusion; regulation under the ECA was to move us from a mindset of natural monopolies and all that goes with that to a convergence mindset with a flat market structure and regulation in the interest of the consumer, finally! But this has not been the case and will not be that case because the regulatory framework still treats the industry like a cash cow for government which ends up with the industry milking the consumer, some more.

# Towards Sustainable Departmental Interconnectivity and E-Delivery for the South African Department of Internal Affairs

**Prof Omphemetse Sibanda, Sr.**
University of South Africa
Pretoria, South Africa
SIBANOS@unisa.ac.za

## ABSTRACT

The problems that besieged the then South African Department of Home (Horror) Affairs are public knowledge and well documented. This is despite the United Nations at one stage having declared South Africa as a country with the best and the strongest e-government capacity in Africa. There is a pressing need for the now renamed Department of Internal Affairs to be saved from inheriting the horrors of the previous administration, particularly in light of the role the Department of Internal Affairs play, in conjunction with the Department of International Relations and Co-Operations, and the Department of Public Service and Administration, as the face of South Africa in the eyes of the international community. In this qualitative research paper a case is made for the expansive use of ICT to enable efficiency gains and act as a tool for public value management in the Department of Internal Affairs. The Department should provide a real around-the-clock people orientated service within the context of the Batho-pele principles. It is hoped that the recommendations in the paper will help in creating a blue-print for other Departments and for the digital South Africa plan. The paper briefly looks at the challenges and problems at the Department of Internal Affairs including human and intellectual capital without necessarily dealing in-depth with the digital divide question; the improved effectiveness, efficiency, and friendliness in service delivery; and the consideration of ethical efficient departmental governance focusing primarily on transparency, equity, rule of law, and gains thereof. Part of the arguments in the paper is that the initial failures of HANIS should be welcome as they demonstrated the dangers of relying on rhetorical discourses of e-government without laying a proper foundation for e-government initiatives. Moreover, the paper looks to the implementation of e-government in local government in Morocco, and also considers the recent Digital Britain Report to draw some valuable lessons. Part of the recommendations made in the paper is that South Africa should create her own model of e-public management and e-delivery for all the Departments. The country should also find the niche for its e-government issues.

**Keywords:** e-Fez Project, digital divide; e-delivery, e-government, e-service, interconnectivity, delivery; ICT, Vision 2014, sustainability.

## 1. INTRODUCTION

### 1.1 ICT as Efficient Government Enabler

As the Internet, and the broader information technology and communication (ICT), becomes part of our daily lives, South African government department have little choice but to embrace it. It perhaps a sense of relieve that the Government of South Africa is committed to seeking to render services using ICT as an enabler, and the reduce the digital divide (Sibanda 2009, p570). For example, the South African government is gradually enabling citizens to access government documents, file taxes, order government publications, and renew licenses and permits using an internet connection. (van Rooyen and van Jaarsveldt 2003, p237). It is therefore no suprise that in 2003? The United Nations ranked South Africa the first and strongest in Africa on e-government capacity (Sibanda 2009, p570); van Rooyen and van Jaarsveldt 2003, p241). The South African government has introduced several projects and initiatives to implement e-government systems, such as the Integrating the Justice Cluster

System;[1] the National Automated Archival Information Retrieval System;[2] tax e-filling; e-procurement; and most importantly for our study the home affairs national identification system (HANIS) project was launched by the then Department of Home Affairs as a tool to combat crime, and also designed as part of the vision by the Department to re-defining its relationship with citizens (Sibanda 2009, p573).

From governance perspective, the deployment of electronic government, that is e-government system, is of great value (Sibanda 2009, p570). In this paper the term "e-government" is used to refer to the use of electronic technology, including e-mails, cellular phones, the Internet and the cyberspace in order to improve dissemination of information and service delivery (Sibanda 2009, p570). Thus, e-government is a system used to support and enhance government activities (See Almagwashi and McIntosh, 2009). In this paper e-Government is to be understood in a broader sense, without having to specifically use phenomenon such as m-government.

### 1.2 Scope of the Paper

In this paper we will specifically appraise the provision of services at the Department of Internal Affairs (DIA), formerly the Department of Home Affairs. Specific study on DIA's e-governance processes is important because of DIAs critical role in the South African government, including particularly DIA as a point of contact with citizens of other countries, who always expect a better service delivery and most importantly its role of record keeping of citizens' life events such as birth and marriage. It is the country's custodian of citizenship that should always run efficiently and effectively using or employing world best practices. In this study we will concentrate particularly on the internal arrangements, operations and management at DIA within the context of e-governance. Though the problem of digital divide[3] pose a challenge to meaningful efforts to place DIA governance into the digital milieu, the problem of digital divide will not be thoroughly be dealt with in this paper as it has been properly and in depth dealt with somewhere (See Sibanda 2009; Tinarwo, Mandioma and Muyingi 2007).

## 2. THE SOUTH AFRICAN E-GOVERNMENT FRAMEWORK

### 2.1 The 2001 e-Government Policy

The first South African e-government policy was drafted by the Department of Public Service and Administration (DPSA) in 2001 (DPSA e-Government Policy, 2001). The policy, based on best international practices on e-government, sets out a ten year implementation plan for e-government,

---

1 This is a gateway project maintained by the Department of Justice and Constitutional development. Part of the project to transform the justice system and process into an integrated, streamlined, modern business system that is supported by ITC, and to that transform the justice cluster into a virtual organisation.

2 National Automated Archival Information Retrieval System (NAAIRS) serves to assist members of the public and other users of national archives to identify and locate archival materials or public records that are relevant to their requirements. As an important tool for electronic service delivery, NAAIRS contains only information about archival material and their documentation and not the actual texts of documents.

3 For the purposes of this paper, we use the term digital divide as refering to a gap between individuals, households, and geographic areas with regard access to information and communication technology (ICT) and to government services delivered through ICT. Tinarwo, Mandioma and Muyingi (2007) reject the application of this basic definition of digital divide in South Africa as "a misfit". They argue that the digital divide in South Africa is as a result of past government's apartheid policies and that lack of access to digital facilities should rather be described as "Digital Wall". This assertion is only correct in part. Separate growth elements are still present and continuing in South Africa in the context of ICT. Past separate development policies should rather be treated as challenges to bridging the digital divide in this paper.

which takes into account the World Summit on the Information Society (WSIS) plan of action on ICT and the 'United Nations' Millennium Development Goals.

### 2.2 Batho-pele Principles and Gateway

The South Africa's e-government policy is also based on the country's "Batho Pele" (in simple English "People First") principles. The Batho Pele is the name given to the government's definitive regulation on public service delivery. In terms of the Batho Pele approach the purpose of public service the efficient and effective service of all the people of South Africa. Through the Batho-pele approach South Africa has committed herself to maximizing service delivery to all the citizens. It calls for the provision and access to service and delivery thereof to anyone, anywhere, and anytime. The Batho-Pele Gateway Portal was launched in 2004 to provide important information including of legislation and policies of the government.

In the spirit of Batho-pele several collective ICT centers, though not truly public centers, have been set up and are operating in South Africa, or planned to operate for the purpose. These include mobile Internet units, and community ICT centers to support special needs and requirements of a particular society (Sibanda 2009, p574). For example, about 800 public information terminals (PIT) have been erected; about 355 Multi Purpose Community Centres (MPCC) have been established for rural communities (Farelo and Morris 2006, p7). The South African Government MPCCs programme were set up as primary vehicles and enablers for the implementation of development communications and information programmes, designed to offer a wide range of community empowerment services (See Jacobs and Herselman, 2005).

### 2.3 Open Source Systems

In February 2007 the Free and Open Source Software Strategy and Policy (FOSS) was approved by the South African Cabinet (Sibanda 2009, p571). The proposal for free and open source policy in South Africa was approved by the government in 2003 (DPSA 2006, p2). FOSS aims at lowering the ICT administration costs and further developing and enhancing IT skills. The FOSS initiatives are in effect administered by the department of science and technology, the Council for Scientific and Industrial Research (CSIR) and State Information Technology Agency (SITA).

### 2.4 ICT Structures

The South African government ICT structure consists of interrelated organs namely: the DPSA, the SITA; The Government Information Technology Officers Council (GITOC); and the National Treasury. These institutions collectively are responsible for the implementation of the country's e-government plan. In particular, DPSA is responsible for the ICT responsibility for national and provincial government including ICT policy making, regulation and strategy formulation. GITOC serves as a forum for consultation and negotiation on ICT issues, and also serves as an advisory body to the Minister of Public Service and Administration on ICT issues. SITA was set up to implement the government's core networks.

There are other supplementary structures, such as, for example, the Universal Service Agency. The Agency was established by the South African Telecommunications Act of 1996 to promote affordable access and universal services in ICTs for disadvantaged communities (Intelecom Research 2000, pp39 -50).

The e-government plan is packaged in six stages, namely: to-way transactions; multi-purpose transactions; personalised portals; clustering of services; and corporate transformation.

### 2.5 ICT Plans and Strategies

Several gateways are established at both central and provincial level of government to serve as a single

point of access to all information about and services which are provided by the government through the use of technology. The aim of the gateway is to create a 24x7x365 responsive online government, which is very conveniently located to the users. And to transform any government service from a manual to an automated system. Several ICT centres and gateways are established throughout the country to address the digital divide problem. Moreover, the Department of Communication has undertaken several projects aimed at making ICTs accessible, including: Internet café's and kiosks; mobile computer stations and satellites dishes. As part of the ICT revolution in South Africa government department maintains websites that provide a range of information, including but not limited to, government documents such as legislation, Bills, commissions reports, research reports, policy documents, government forms, and other government notices. South Africa has nine provinces each with its e-government strategy and ICT gateway.

Strategies have also been put in place to introduce and/or increase universal access to ICT. For example, small medium enterprises (SMEs) have been granted Under-serviced Area Licenses (USALs) to provide ICT services is designated areas (Gilwald 2005, p6). This project is to be understood alongside Universal Access Funds (UAFs), which is operational in South Africa used as incentives to ICT operators to distribute telecommunications access into pooper and less profitable areas of the community. Through UAFs, or smart subsidies as it may be called, South Africa followed a practice in several countries including the United States.

### 2.6 Legal Framework

The South Africa's e-government legal framework includes, but is not limited to: the Electronic Communications and Transactions Act of 2002. ECTA was assented to on 31 July 2002 and came into operation on 30 August 2003. According to the preamble of the ECTA one of the purposes of the Act is to "encourage the use of e-government services." Chapter 4 of the ECTA specifically deals with or makes provision for e-Government services; Telecommunications Act (SATA) of 1996, which amongst others seek to promote the universal and affordable provision of ICT services; make progress towards the universal provision of ICT services; encourage investment and innovation in the ICT industry; encourage the development of a competitive and effective ICT manufacturing and supply sector; and most importantly, to promote the development of ICT services responsive to the needs of users and consumers, including disabled persons; to encourage ownership and control of ICT services by persons from historically disadvantaged groups; the Public Service Regulations (PSR) of 2001. The principles contained Chapter 5, Part I, of the PSR specifically requires department to manage ICT efficiently and effectively taking into account the Batho-pele principles. Part III sets interoperability standards, which at a closer look will enhance citizen access to ICT services and also contribute immensely towards bridging the digital divide; and the Electronic Communications Act (ECA) of 2005 is a one of the ICT specific legislation in South Africa. In addition to the stated aims of promoting the convergence the ICT sector, ECA regulates the provision of ICT services and of electronic communications network services and broadcasting Services.

## 3. SAMPLE OF SPECIFIC DIA E-GOVERNMENT RELATED PROJECTS AND INITIATIVES

### 3.1 Network Interconnectivity

Part of the overhauling of service at DIA has been the consideration of office connectivity to address connectivity and standardize on infrastructure in order to improve service delivery, increase end-user productivity, eases support and maintenance, enhances reliability, and improves security controls. To this end DIA has embarked on the process of implementing a new network infrastructure in partnership with the Department of International Relations and Co-operations. The network infrastructure is designed also introduce a single point of access ie. network operating center.

### 3.2 National Automated Fingerprint Identification System

HANIS project was launched as part of the vision by the DIA to re-define its relationship with citizens. Part of the project online provision of services, for example, the making accessible birth and death registration forms on line. It is a biometrics-reliant automated identification system comprising of three components, namely: automated fingerprint identification system, system integration and identity card. One of the potential uses of HANIS includes elections, population verification and registering, and us by the immigration authorities. HANIS works almost the same as the National Automated Fingerprint Identification System (NAFIS) of Australia, which assists police across Australia to establish identity from fingerprint and palm impressions quickly and reliably to help solve crimes. NAFIS is monitored, maintained and enhanced to continue meeting long-term police needs, including the ability to integrate new digital input and output devices.

The related project is the HANIS Back Record Conversion Project, which was initiated to scan and absorb the approximate thirty million hard copy fingerprint records. The record conversion project aims also to address the problem of multiple identity documents in that it seeks to ensure that a person only comes into possession of one identity number.[4]

Records conversion is part of the electronic management system, which has inherent pitfalls and should be properly employed. The jury is still out on DIA's performance in this regard. It is hope that citizens' records or data will not be lost in the conversion process.

### 3.3 Integrated Electronic Management System

On the 15th of December 2006 the DIA published a tender for the implementation of the integrated electronic management system (IEDMS). The objective of the IEDMS is to implement an effective online solution that will cater for automated document management processes from capture to business transaction completion resulting in the overall improvement of business process efficiency. The objective is to reduce manual paper-driven environment; improve service delivery; and eradicate storage problems.

Migration to paper-less environment is to introduce online interface system. Part of the system is to implement online registration. The benefits that the system aims to bring are manifold, including: improving turnaround times for documents applications; improving security; improving integrity through the enforcement of business rules. From the fast and effective service delivery point of view the move has been to introduce the General Live Capture Concept (GLCC) with Highly Configurable Counters housing Integrated Client Service Consoles (ICSC) backed by Fault-tolerant Controllers for offline processing at any office in order to address the office counters and queuing.[5]

### 3.4 Business Intelligence and Data Warehouse Project

The business intelligence and data warehouse project (BI) is essentially a project aimed at information dissemination. The objectives of the BI project are to provide a consolidated view of all information sourced from existing systems by establishing a data warehouse and to provide business intelligence tools to access, analyze and report on data in the data warehouse.

BI came as a result of data challenges experienced by DIA including the departmental systems operate in silos; fraudulent activities due to lack of integration; lack standard operating procedures in respect of information that is captured; employees not understanding the importance of their functions and the impact of their roles on managerial decision-making; and the lack of universal view of a person at DIA.[6]

---

4 See generally DIA website.

5 See generally DIA website.

6 See generally DIA website.

## 4. SOME PROBLEMS WITHIN DIA

At least DIA has acknowledged that there are problems it has to deal with, and intervention processes were considered in 2006 to address these problems.[7] In respect to the implementation of e-services by the DIA the following are worth to mention:

### 4.1 High Criminal Activities

A host of problems including different identity documents, the volumes of manual fingerprint system of about 37 million records, and the high incidence of fraud in welfare, health, housing and manpower.

### 4.2 Ineffective Manpower

The country continues to experience the brain drain in the ICT sector. Economic factors have resulted in the country looking skilled ICT personnel, who are given more attractive salaries and incentives by private companies and other countries. It therefore means that the e-government programme is left with having to do with less skilled workers (Sibanda, 2009, p576). The teething problems experienced when DIA introduces HANIS bears testimony. In fact, the lack of ICT skilled human capital retards the progress towards ICT culture and bridging the digital divide. Speaking generally, ICT analysts have predicted that ICT industry may suffer about 25% loss due to skills shortage. One of the reasons is that the country supply skills inadequate to satisfy the demand.

A casual walk into one of the DIA offices and approaching one of the employees will immediately point towards inefficient. Part of the problem at DIA the customary practices and doing businesses as usual, which is a serious hurdle in the implementation of e-processes at DIA, and in other government departments.

## 5. LESSONS FROM MORROCO

### 5.1 Morocco

#### 5.1.1 General

Morocco is one of the African governments that have successfully implemented an e-government project, particularly at local government level. The relevant example is the eFez Government Pilot Project by the City of Fez, in which ICTs services were introduced specifically in the city of Fez in the Civil Registry Offices, which are government offices officially known as "*Bureaux d'Etat Civil*" (Kettani *et al* 2008, p.1). The Civil Registry Offices is the local government equivalent of the DIA. The eFez Project has been hailed as a success story and a lot of the success can be attributed to the firm foundation laid for the implementation of e-government, which DIA and South Africa in general can learn from. Like DIA, the Civil Registry Offices are responsible for the keeping of records of citizens' life events such as birth, death, marriage, divorce, and others (see Kettani *et al* 2008, p.1).

The eFez pilot project has won few awards on e-government, namely: the national eMtiaz Prize (Prize of Excellence) for the best electronic administrative service in Morocco; the Award of Technology in Government in Africa (TIGA) for the category of Regional or Provincial electronic government services; and the UN Public Service Awards 2007.

---

[7] See 'Super-squad' to fix home affairs in 6 months" *Cape Argus* 14 July 14, 2006: Online **http://www.iol.co.za/index.php?set_id=1&click_id=13&art_id=vn20060714122132143C615**

### 5.1.2 Phased Project Implementation

The project was introduced and implemented through phases. The first phase involved amongst others the promotion of good governance, the development of local capacities and research on how to improve access to social services. The feaseabilty study was conducted to prove the need for offering citizens electronic services that provide easy access to important documents. The phase considered the digital divide challenges. The implementation of the e-government services considered the needs and capacities of citizens taking into account their educational level, their familiarity with computers, and the availability of ICT services in local languages. The issue here is that on-line services are an extension to the face-to-face services aiming to improve the quality of services to citizens, and should be as accessible as possible and be user-friendly.

The process of introducing ICTs into the Civil Registry Offices of the city of Fez required several changes to be realised such as the training of the employees; the adjustment of physical spaces of work within civil Registry Offices; redeployment of personnel, and where employees were retained their tasks and responsibilities were indicated; transparency was emphasised as an integral part of good service delivery; and the public spaces are transformed into open spaces.

The e-Fez resulted in the City of Fez replacing manual service delivery with automated service delivery at both the back office and the front office desks. The automated service delivery is supported by , amongst others, self-service touch screen kiosk, and online access portals (Kettani *et al* 2008, pp.11 -12). According to commentators (Kettani and El Mahdi 2009, p395) have greater expectations in regards delivery and efficiency of the protocol at Civil Registry Offices in Fez. Part of the values generated by the eFez Project include efficiency gains for the Civil Registry Offices' administration, and infusion of public value in Civil Registry Offices' institutional governance(Kettani and El Mahdi 2009, 2008, p396).

The important feature of the eFez Project lies with its objective of enhancing stakeholders' readiness and awareness. Many e-governments projects failed because of the lack of institutional, infrastructural, and human capital readiness. The top-to-bottom implementation is not always the solution. A mixed e-government implementation is the good approach.

## 6. CONCLUSION AND RECOMMENDATIONS

### 6.1 Conclusion

The Promotion of Access to Information Act of 2000 places an obligation on e-government services to be more accessible, including taking appropriate steps to bridge the digital divide particularly in cases where the services are offered primarily or substantially through ICT facilities. Fortunately, the South African government has joined the rest of the world in making use of the information age to deliver effective, efficient and high-quality services to its citizens. There is in principle an acknowledgement that e-government approaches positively transforms the manner in which government institutions, citizens and business and public employees interact with the government. There is a clear acknowledged that ICT can strengthen the effectiveness of good governance and broaden the participation of the society in governance process. The South African government has also set up appropriate institutional and legal frameworks and policies to make e-governance a reality. If ICT can increase the productivity, efficiency and market reach of firms (Criscoulo and Waldron 2003); the same should be experienced in government. The DIA is one of the South African Government Departments that have experienced serious problems in service delivery, and is gradually making good efforts to discard its image as a problem riddled Department.

### 6.2 Recommendations

The lesson learned from the eFez project is that narrowing the digital divide and laying a proper foundation to the implementation of ICTs services is important to the success of e-government. As a good model for e-government the eFez provides is an example of how citizens' oriented ICTs services can be successfully implemented. The essential characteristics of the eFez Project providing citizens with "transparent, empowering, efficient and effective access to services on an equal basis, and providing a means to ensure accountability and impartial application of the law and in this way contributing overall to local "good governance" in Morocco" (Kettani *et al*, 2008, p18).

South Africa has serious challenges related to ICTs, which will impact on individual Departments' e-governance processes. Such challenges, which need to be addressed, include: communities' economic differences and Ownership of ICT Products. Not many South African household own a complete ICTs infrastructure the marginalization of rural areas in ICTs development. These are the communities who most struggle to access DIA services. The plight of these communities will remain on the digital divide side the infrastructural, social and technical challenges involved are allowed to continue unresolved (Sibanda 2009, p774); linguistic barriers are also a challenge to DIA progress in the implementation of ICTs. It is not encouraging that in a country with 11 constitutionally recognized official languages the country's internet/ICT content is influence by preference to English (and Afrikaans) (See Sibanda 2009, 575). If one browses DIA website you will realise that the content is 100% English. DIA like many of the other Departments fail to recognize that English is not the first language of majority of the South African population. Where it is spoken by non-English people only a sizeable number of South African can speak, read and write English fluently (Sibanda 2009, p575); language barrier is compounded by the challenge of computer illiteracy. It is one thing to advocate accessible and affordable ITC structures and programmes, but it is another to expect the use of such structures or facilities without the necessary and appropriate training and education.

It is therefore recommended:

- Technology is forever transforming itself and DIA must respond to the new ways of doing business. The citizens' demand for government services to match the private sector in every way.
- Before DIA undertake the transformation of its public services it must transform its approach to sustainable IT enabled business change. E-delivery and e-information will contribute towards solving many of DIA's problems.
- DIA must improve its back-office, middle office, and front office processes and presentation. It should always be remembered that the wrong start end it explosive wrong results.
- DIA having benchmarked e-governance and e-services as its priorities should revisit its implementation strategies. A lot can be learned from projects like the eFez Project IN Morocco. Lesson can also be learned from the Egyptian model towards bridging the digital divide. A study conducted by Maha (2008), reveals that Egypt is one of the few African countries that achieved great development in ICT services and access. Egypt uses the so-called Feasibility for Initiatives Adoption, Implementation, Feedback, Moderation (FIAIFM) models, which "provides the mechanism for identifying areas needing improvement and provides guidelines that could be followed" (Maha 2008, p12). It is through the processes involved in this model that a national programme called "Egypt PC 2010 – Nation Online" has been established (Maha 2008, p12).
- DIA introduce or develop ITC software in other local languages to make its website more accessible. Lack of African languages software is a barrier that prevents full access and enjoyment of services and of exposure to DIA's e-services.
- The ITC education and training of DIA employees should be prioritized. In particular, the

> employees should know how to use the relevant ICT applications and programmes which are part of DIA's e-governance processes.

Of course DIA efforts cannot be incomplete clinical isolation from the national e-government implementation drives and is not immune from national e-government challenges. Some of the issues will need to be dealt with by the national government in order to enable individual Department to carry through their e-government projects. Perhaps one should mention the need for the national government to promote a viable and realistic ICT access programs for rural areas promoting the meaningful involvement of communities in ICT revolution (See Sibanda 2009, p577; Conradie and Jacobs 2003, p33); and promoting viable ICT access; encouraging private sector and ICT practitioners' participation in the ICT revolution; utilise alternatives to broadband to overcome infrastructural barrier by using alternative access means such as broadband powerline (PLC) at a larger scale (Sibanda 2009, p577. See also Tinarwo, Mandioma and Muyingi 2007; Thomason 2006, p2). To this end the government will need to undertake a comprehensive and holistic programme to digitalise its services and enable all stakeholder to use its services. The "Digital Britain" efforts may be used as an example of how we should go about doing this. The "Digital Britain" project is an ambitious project whose programme of action proposes several interesting initiatives. This include (1) ensuring that citizens have the capabilities and skills to meaningfully participate in the digital environment, and (2) expecting government to modernize and improve its services to citizens through digital procurement and digital delivery of pubic services (*Digital Britain Report* 2009 p1). Of particular interest in the context of this study in Chapter 8 of the Digital Britain Report and recommendations therein. The Chapter speaks to several issues including migration to digital government and benefits thereof (*Digital Britain Repor*t 2009, pp207 – 209), and the proposed digital switchover of public service programmes (Digital Britain Report 2009, p210). South Africa can learn a lot from Britain in introducing a sustainable national digital plan.

**REFERENCES:**

Arntzen, J, Krug, D, and Wen, Z. (2008), "ICT Literacies and the curricular conundrum of Batho-pele Handbook [Online], http://www.dpsa.gov.za/documents/gics/bphb/BathoPeleHandbook.pdf

Bello, H.M. (2003) The role of information and Communication technology in the fight against poverty – the: Nigerian Experience, Paper presented at the Symposium on ICT and the Society Information, 9th – 11th December 2002, Algiers, [Online], http://allafrica.com/stories/200301200386.html

Conradie, D.P. & Jacobs, SJ. (2003) "Challenges encountered when using ICTs in support of development in rural African communities", Engineering Management, 30 – 33, February 2003.

Department of Culture, Media and Sport and Department for Business, Innovation and Skills (2009) Digital Britain : Final Report (presented in Parliament on July 2009)

Department of Public Service and Administration. (2006) "Policy on Free and Open Source Software Use for the South African Government", [Online], http://www.dpsa.gov.za/documents/ogcio/2007/FOSS_OC%20POLICY_2006_APPENDIX%20A.pdf

Thomason, D. (2006) A Multipath Model for the Powerline Channel, [Online], http://www.ele.auckland.ac.nz/archives/reports2005/pdfs/Telecommunications/proj_025_dtho086.pdf

Farelo, M and Morris, C. (2006), The Status of E-government in South Africa , pp 1 – 12, [Online], http://researchspace.csir.co.za/dspace/bitstream/10204/966/1/Farelo_2006_D.pdf

Gilwald,J. (2005) "A Closing Window of Opportunity: Under-Serviced Licensing in South Africa", The Massachusetts Institute of Technologies and International Development, Vol 6 Number 4, pp1 – 19, [Online],

http://dev-ejournals.library.gatech.edu/redesign/index.php/1111/article/view/391/307

Jacobs, S.J, and Herselman, M.E. (2005) "An ICT-Hub Model for Rural Communities", International Journal of Education and Development using ICT, Vol 1, No 3, [Online], http://ijedict.dec.uwi.edu/viewarticle.php?id=58&layout=html

Galvin M. (1999) "The impact of local government on rural development in South Africa", Transformation Vol 40, pp 87 – 112.

Grimsley M and Meehan A. (2008) "Attaining Social Value from Electronic Government" The Electronic Journal of e-Government, Vol 6 Issue 1, pp31-24 at 31.

Intelecon Research. (2000) The use of information and communication technology (ICT) in learning and distance education, [Online], http://www.col.org/colint/00intelecon.pdf.

Kettani, D, Moulin, B, Gurstein, M, and El Mahdi, A (2008) " e-Government and Local Good Governance in Fez, Morocco" The Electronic Journal on Information Systems in Developing Countries, Vol 35, pp 1 – 18.I

Kettani, D and El Mahdi, A (2009) "Fe e-Government Project: An Initiative Transforming Scientific Research to Value in Morocco" in Hamis, P and Remenyi, D (eds), Proceedings of the 9th European Conference on e-Government, 29 – 30 June 2009, Academic Publishing Limited : Reading, UK.

Kroukamp, H. (2005) "e-Governance in South Africa: are we coping", Acta Academica, Vol 37(2), pp 52 – 69.

White Paper on Transforming Public Service Delivery, Notice No 1459 of 1997, [Online], Department of Public Service and Administration (South Africa), http://www.info.gov.za/whitepapers/1997/18340.pdf

World Summit on the Information Society. (2003), Geneva/Tunis Declaration of Principles and Plan of Action, Document WSIS-03/GENEVA/DOC/5-E (12 December 2003), [Online], WSIS,

http://www.itu.int/wsis/docs/geneva/official/poa.html

Van Rooyen E.J and van Jaarsveldt L.C. (2003) "A South African Development Perspective on e-Government" Journal of Public Administration, Vol 38, No 3, pp 237 –pp 252.

Tinarwo , L, Mandioma, M, and Muyingi, M. (2007), PowerLine Communications an Integrative Solution to Digital Divide and Broadband Delivery for the Non-Broadband Communities of South Africa, [Online], http://www.satnac.org.za/proceedings/2007/papers/access/Paper%2072%20-%20Tinarwo.pdf

Sibanda, O (2009), "e-Government in South Africa: Successes and Challenges in the Quest to Bridge the Digital Divide" in Hamis, P and Remenyi, D (eds), Proceedings of the 9th European Conference on e-Government, 29 – 30 June 2009, Academic Publishing Limited : Reading, UK.

Almagwashi, P and McIntosh. S (2009), "Understanding the Government to e-Government Transition Using a Soft Systems Approach: What is e-Government Supposed to do? in Hamis, P and Remenyi, D (eds), Proceedings of the 9th European Conference on e-Government, 29 – 30 June 2009, Academic Publishing Limited : Reading, UK.

# Cybersquatting and Domain Name Dispute Resolution: Affirming the Bundle of Rights Theory

**'Dejo Olowu**
Professor of Law, School of Law
Walter Sisulu University
Nelson Mandela Drive
Private Bag X1
Mthatha 5117
South Africa
*Phone:* +27-73-241-3815
*Fax:* +27-86-573-2740
*Email:* djolowu1@yahoo.co.uk.

**ABSTRACT**

When a corporate organization registers its trademark, logo, or business name as its domain name, traditional understanding of property law would lead such an organization into believing that it retains the right to the use of that domain name to the exclusion of any other person or entity. But what happens when someone else registers the trademark, logo or business name of another as domain name before the actual owner applies for domain name registration? Or what is the position of the law where someone deliberately omits, adds or misspells a letter in an existing domain name and proceeds to register it as a distinct domain name? On what basis would or should the law intervene to protect the interest of the original domain name user? While the phenomena of cybersquatting and typosquatting have received some considerable attention in scholarly works as well as juridical decisions across various jurisdictions, there remains a paucity of discussion on the underlying philosophical basis for protecting the interests of one party against the other. Beyond the traditional application of common law property rights to cases involving cyberspace infringements in general, this paper particularly accentuates a legal basis for the protection of proprietary interests against cybersquatters and typosquatters. Reflecting on juridical disputes from diverse jurisdictions, this paper demonstrates that the bundle of rights theory, an idea that had received much vilification and polarized jurists particularly in Anglo-American legal traditions, provides the most plausible philosophical foundation for tackling the menace of cybersquatting. The paper then investigates the practical significance the bundle of rights theory, among other proprietary concepts, has for the issue of Internet domain names, and in reconceptualizing our understanding of the boundaries of proprietary *res* in a novel environment.

Keywords: Domain names, cybersquatting, typosquatting, property rights, bundle of rights.

## 1. INTRODUCTION

Although originally designed to serve the objective of military defense, there is no gainsaying the fact that the Internet has metamorphosed into the superhighway of information providing an unprecedented marketplace for all manners of business and drawing millions of prospective users. But with the tremendous growth of the use of the Internet for commercial purposes has risen a wide range of challenges far beyond the contemplation of its designers. Since the advent of the commercial usage of the internet, there has been an exponential growth in the way society perceives and conducts the business of communication, entertainment and trade. In the age of the internet, therefore, it has indeed become commonplace for small, medium or large business entities to seek the registration of their business names, logos, trademarks or other insignia that would identify their products and services among their targeted audience. A company would thus naturally identify and distinguish itself on the

Internet by registering a domain name, usually a well-known name or a registered trademark. The manufacturers of Coca Cola would, for instance, be keenly interested in having the words "Coca Cola" or "Coke" as their registered domain names, with the expectation that they will be protected against infringement. While the foregoing illustration would appear straightforward, the reality of internet age commerce manifests numerous challenges and complications that had not been foreseen.

Domain name registrations are allocated to persons by paying a nominal fee and filling out registration forms on the basis of 'first come, first served', regardless of any trademark rights vested in the name, and therefore, there is no mandatory authentication of existing trademark rights in the words constituting the domain name (Chalikian 2001). Since two domain name registrants cannot have two domain names spelled the same way, there had been an increasing trend of individuals registering many well-known trademarks as domain names, with the intent to resell to the owners of the existing proprietary rights. This phenomenon is known as cybersquatting. We shall consider this as well as its variant, typosquatting, in detail shortly.

Across various jurisdictions, the courts, as well as similar bodies, have repeatedly had cause to intervene in matters pertaining to rights over domain names. However, despite the overwhelming number of decisions on lawsuits arising over domain names, there is no plausible indication that such lawsuits would end. While adjudicatory bodies have addressed the problem of cybersquatting by applying traditional trademark laws to claims against domain name infringements, it is becoming evident that even a decade into the twenty-first century, conventional trademark and property laws are proving inadequate for providing remedies in the Internet arena.

Although various approaches have been canvassed on the legal dilemmas encountered in tackling cybersquatting, this paper proceeds from the assumption that there is a missing philosophical link in the way legal practitioners and researchers conceptualize the basis for remedying infringements of domain names, namely, within the narrow confines of trademark law.

While not underestimating the skepticism that a critical approach to the dominant juristic view might generate, I advance an alternative justification for the protection of rights in domain names through a re-exploration of the bundle of rights theory, establishing a different philosophical foundation for conceptualizing domain names as integral incidents of property rights.

## 2. SIFTING THE MATRIX OF TERMINOLOGIES

Because some level of familiarity with the Internet is necessary in any discussion of infringements in cyber matters, this segment provides a brief overview of the structure of the Internet with particular attention given to the notion of domain names, how domain names are assigned; cybersquatting and typosquatting as related infringements of the cyberspace as well as an overview of the bundle of rights theory.

### 2.1 The Domain Name System

By all standards, the Internet is comparable to a telephone system. In the same way every telephone is assigned a unique number, so is each computer on the Internet also assigned a unique number. By entering this number, referred to as an Internet Protocol (IP) address, into a web browser, Internet users are able to access information contained on the corresponding computer. This information is displayed by way of the use of web pages. Generally, a web page may contain text, graphics, audio, video, or any combination of these elements. A group of web pages that are maintained as a single informational source is referred to as a website. Because entering a long IP address can be unwieldy, the use of domain names was promulgated early in the development of the Internet (Greenberg 2004).

Domain names are comprised of alphanumeric characters. This sequence of alphanumeric characters is then correlated to a website's IP address. As such, an Internet user can access a particular website by entering a readily cognizable alphanumeric combination instead of a lengthy sequence of numbers. It will thus be much easier for a web surfer to type in www.wsu.ac.za than to remember its IP address of

196.24.29.41.

In particular, a domain name is a composite of both a top-level domain name (TLD) and a second level domain name (SLD). A top level domain name may be either a country TLD or a general TLD. As the name suggests, a country TLD is assigned to a particular country. That country is then allowed to determine who may utilize their TLD. In contrast, general TLDs are not associated with any particular country and are intended to signify the type of organization that is operating the website. Unfortunately, with the exception of the ".mil"; ".gov"; and ".int" TLDs, there are no restrictions on who may utilize a particular general TLD. Therefore, the operator of a given website may not, in actuality, be the type of organization signified by the TLD (Cotton 2002). This lack of screening by the domain registry makes it easy for a competitor to either reserve a domain name using an existing mark not already reserved by a trademark owner, or by using a domain name which is deceptively similar to an existing trademark.

In contrast to the TLD, which is the same for numerous websites, an SLD is a unique alphanumeric combination that may only be assigned to a single website within each class of TLD. Terms that reflect the nature of the website are often chosen as the SLD. For instance, it is not uncommon to find a company using its name as its SLD. In this manner, there is an impressionable link between the company and its domain name. As an example, a visitor to "cnn.com" may readily verify that the Cable News Network has chosen "CNN" as its SLD and ".com" as its TLD. The use of the domain name "CNN.com" therefore reflects the identity of the website operator, the Cable News Network, and the fact that the operator is a company. Gole (1999: 406) sums it up as follows:

> A domain name is an easy-to-remember replacement for an Internet address. When an individual or corporation registers for a domain name, it is actually assigned an Internet Protocol (IP) address such as 169.229.97.112….Because IP addresses are difficult to remember, Internet users substitute unique "domain names" as pseudonyms for the computer's real identification number. When a domain name is entered into a computer it is automatically converted into the numbered address, which contacts the appropriate site.

### 2.1.1 Acquisition of Domain Names

As the commercial use of the Internet grew in the 1990s, many companies began registering their names and trademarks as domain names on the Internet. As commerce increased through the Internet, the value of domain names rose. Because registration for domain names has always been on a "first come, first served" basis, individuals who were fast enough could register domain names before the original mark owners had the opportunity to do so. Upon securing ownership of the names, many would then attempt to sell them to the owners who often spent millions of dollars developing the goodwill of the trademark (Efroni 2003; Gusewelle 2004). Since the possession of a trademark does not automatically confer ownership or the exclusive use of the same word or phrase as a domain name, a trademark owner must register its trademark with the Internet Corporation for Assigned Names and Numbers (ICANN), created by the Department of Commerce in 1998, to secure such ownership and use (Gilwit 2003; Gusewelle 2004). The enormous importance of the US government in the registration and control of domain names should be understandable as it played the leading role in the development of the internet.

While no single entity controls the multitude of computers that comprise the Internet, the assignment of IP addresses, and invariably, their corresponding domain names is under the control of the ICANN. Members of the Internet community established ICANN, a non-profit corporation, as a direct response to a U.S. Department of Commerce initiative (Litman 2000). The goal of ICANN is to "privatize the domain name system (DNS) in a manner that increases competition and facilitates international participation in its management" (ICANN 1999). The actual assignment of IP addresses and domain names is performed by private companies that are licensed by ICANN for this purpose. These

companies are referred to as registries. In general, domain names are granted on a first to request basis, that is, the first person to request a desired domain name from one of the licensed registries is usually awarded that name. It is important to note that the registries require no proof that the requested domain name will not violate another's trademark (Holland 2005).

Based on governmental requirement, ICANN established its Uniform Domain Name Resolution Policy ("UDRP") in February 1999 to deal with all incidents of domain name infringement.[i] Under paragraph 2 of the UDRP, every registrant warrants to submit to mandatory arbitration under the UDRP if a complaint is made under the UDRP about the registration of one or more relevant domain names. Although the UDRP process is the subject of vehement criticism and lofty commendation in numerous scholarly works, I shall consider its elements in detail as we go on in this presentation.

### 2.1.2 Domain Name Dispute Resolution

Before 1995, there was no system specifically planned to address domain-name disputes, a reality that compelled aggrieved persons to seek remedy through traditional litigation (Belczyk 2002). The earlier litigants were therefore trademark holders seeking judicial redress against domain name registrations that infringed their trademarks (van der Merwe 2000). Domain name disputes are now often resolved using the UDRP process. A vehemently debated topic is whether the UDRP process favors large corporations and if UDRP decisions are over-reaching. Under the UDRP process, remedies include having the infringing domain name deleted (giving someone else the opportunity to register the just-deleted domain) or transfer of ownership of the domain. Advocates of UDRP maintain it is a faster and less expensive means of dispute resolution than traditional litigation (Lipton 2005; Jones 2007).

Domain name disputes can also be tried in court, however, like other forms of litigation related to the Internet, establishing jurisdiction is often difficult since no consensus has emerged whether the proper place for a case is that of the plaintiff, the defendant or the location of the server through which the domain is registered and serviced.

Lipton (2005) argues that one lingering problem is that the current dispute resolution mechanisms are focused on the protection of commercial trademark interests, often to the detriment of other socially important interests that may inhere in a given domain name.

If the global information society continues down the current road of protecting these interests at all costs, other important social norms relating to Internet use will not have a chance to develop, and the Internet will become permanently skewed in favor of commercial trademark interests. Society may therefore lose out on the potential of developing the Internet in general, and the domain name system in particular, in new and useful ways. What more? Even in the realm of purely commercial interests, the current domain name dispute resolution mechanisms are to some extent deficient. While existing mechanisms such as the U.S. Anti-Cybersquatting Consumer Protection Act ("ACCPA") and the UDRP are extremely useful and effective in protecting trademark interests in the context of bad faith cybersquatting, they are quite limited in their ability to deal with disputes between two legitimate holders of similar trademarks with respect to a corresponding Internet domain name.

It will be apt to mention that while UDRP is fast becoming a global alternative dispute resolution procedure, the nomenclature assigned to it vary across jurisidictions.

## 2.2 Cybersquatting and Typosquatting

As already mentioned above, because domain names are registered on a first-come, first-serve basis, and because domain name Registrars do not check whether applicants possess the right to use the trademark as a domain name, it becomes possible for a person to register a trademark owner's name or mark as a domain name without a bona fide claim to use the trademark. When a person so registers a domain name with intention to sell the domain name back to the owner of the registered trademark, that registrant is deemed to be a cybersquatters. The ACCPA defines cybersquatting as the registering

of, trafficking in or use of a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else.[ii]

Records abound of how many prominent trademarks including those of Panasonic, Coca Cola, Washington Post, and many other conglomerates had fallen victims of cybersquatting. Even notable law firms were not spared of cybersquatting skirmishes in relatively recent past (Jones 2007).

Woollacott (2000) and Cotton (2002) had identified three main categories of cybersquatting, namely, (a) registering a trademark as a domain name with the purpose of extorting money from the trademark owner; (b) registering a domain name very similar to that of a trademark in order to lure Internet users on the off-chance that the users misspell the name they are seeking; and (c) registering a domain name but not making commercial use of the domain name.

The first category consists of those labeled "ransom grabbers" (Mercer 2000: 16; Cotton 2002: 296) as the sole purpose of registering a domain name is to compel the true owner of the trademark or name to part with money. One notorious US cybersquatters, Dennis Toeppen, had reserved hundreds of domain names corresponding to well-known trademarks, waiting for the trademark owners to negotiate his discontinued use of those domain names (Golinveaux 1999).

The second category consists of those labeled "competitor grabbers" (Mercer 2000: 16; Cotton 2002: 297) as one of their main purposes is to encumber the trademark holder's use of the domain name: they register a domain name very close to the name of a trademark or an individual's name, usually by misspelling the name or adding a hyphen (such as adiddassport.com or brad-pitt.com).

The third category involves "domain name warehousing" (Woollacott 2000: 29; Cotton 2002: 297), so named because the registrant registers multiple domain names containing trademarks which he will not make use of in the expectation that the trademark owner would approach him to bargain for the release of the domain name.

The practice of permitting domain names to be registered on a first-come, first-served basis had undoubtedly compounded the domain name infringement problem. The registration system encourages unscrupulous persons such as cybersquatters to beat out a rightful trademark holder in the registration process so that they can take the domain name hostage and request reparation from the trademark holder. This fundamentally threatens the most basic objectives of trademark law (Gilwit 2003). An item bearing a trusted trademark allows a purchaser to easily and immediately determine that item's quality, history, and dependability. Trademark law thus ensures that a producer, and not its competitor, will receive the rewards of goodwill associated with a desired product. Domain name infringement by cybersquatters also weakens the fundamental trademark principle of consumer protection by permitting ruthless competitors to benefit from the mark holder's good will and reputation.

Closely related to cybersquatting is the phenomenon known as typosquatting, involving the registration of domain names that are minor typographical variations on well-known trademarks or names in which the registrant lacks any legal right (Gusewelle 2004). This usually involves deliberate omissions or misspelling of the established trade name. Marsh (2002) asserts that typosquatters attempt to profit from the fame of another's mark and do not generally intend to transfer the infringing domain name to the mark holder or other interested third party. Gusewelle (2004) characterize typosquatting as calculated to divert unwary prospective surfers to advertisements or images that they never anticipated. Once again, no scholarly discussion on typosquatting would be complete without referring to the mind-boggling activity of John Zuccarini, arguably one of the most outstanding typosquatters ever known. Zuccarini had registered more than 3,000 domain names that were misspellings of well-known company names and brands, television shows, important personalities' names and movies from which he reportedly earned about US$ 800,000 to US$ 1,000,000 annually until the long arm of the law caught up with him in several litigation (Jones 2007).[iii]

While there may be validity in Hale's suggestion that the slow or reluctant attitude of many owners of well known marks to accept the Internet as a potential commercial avenue, allowing others to register

domains reflecting their marks gave rise to the problem known as cybersquatting, it remains problematic that at a time when most established trade names and marks have been registered as domain names, cyber con-artists continue to configure registered domain names in a manner that registrants did not anticipate. Although the courts and other dispute settlement mechanisms are fairly responding to the phenomenon of cybersquatting in general, a lingering challenge remains how to balance the interests of contending parties.

### 2.3 Bundle of Rights Theory

In the mid-18th century, English lawyer, William Blackstone, had defined property as "that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe" (1765-1769: 2). To Blackstone, therefore, property is to be conceived as right *in rem*, connoting the exclusive right of the claimant against the whole world. According to this conception, it was not sufficient that an individual claims dominion over property, it was essential that property also entailed the exclusion of other individuals' rights over the same resource.

Blackstone's understanding of property was to become the reference point in property discourses among generations of legal philosophers. The idea of exclusion, in one form or the other, tends to inform almost any understanding of property, whether private, public, or community. The only variation tends to be the person or group in whom it is vested. Private property entails vesting it in an individual; public property, in a government or other agency on behalf of a wider set of individuals; and community property, in members of a community against non-members. Consequently, the tendency among scholars, courts, and legislators to equate conceptions of property with the notion of exclusion remains pervasive (Strahilevitz 2006; Balganesh 2007). So engrossed with the exclusionary conception of property that Thomas Merrill (1998) argued that the "right to exclude" remains the *sine qua non* of property.

At the turn of the 20th century, Hohfeld had developed a novel methodology of understanding legal relations, using what he called "jural opposites" and "jural correlatives" (Hohfeld 1913-1914; Hohfeld 1916-1917; Hohfeld 1923). Using a matrix consisting of rights, duties, privileges and a fourth variable (i.e., the no-right), in his series of works, Hohfeld vigorously made the case for a consistent model of judicial analysis of *in rem* and *in personam* legal relations. The crux of Hohfeld's thesis in relation to property was that property consisted of a large mix of jural relations (i.e., rights, duties, privileges, etc.), not all of which could be mapped at any given point of time. In Hohfeld's analysis, a right (or a claim) is defined as a situation that places another individual (or group of individuals) under some sort of correlative duty. The content of the right is defined entirely by the content of the correlative duty (or obligation) that it imposes on another. Hohfeld contrasts his idea of a right with that of a privilege, which has independent normative content in that it *privileges*, or allows its holder to do certain things, quite independent of others. Its correlative is thus a "no-right," a position that represents the absence of a right in anyone else to stop the holder's privileged (or allowed) action. Hohfeld makes the distinction most obvious with the illustration of landowner X, noting that "X has a right against *Y* that he shall stay off the former's land" and, equivalently, "Y is under a duty toward X to stay off the place." He further observes in the context of the right-privilege distinction that "whereas X has a *right* or *claim* that Y, the other man, should stay off the land, he himself has the *privilege* of entering on the land."

Complementing Hohfeld's analysis was the list of the "incidents" of ownership described by Honore in his seminal work titled "Ownership" (1961), in which he set out the eleven quintessential elements of ownership. According to him, these include: (i) the right to possess; (ii) the right to use; (iii) the right to manage; (iv) the right to the income of the thing; (v) the right to the capital; (vi) the right to security; (vii) the incident of transmissibility; (viii) the incident of absence of term; (ix) the duty to prevent harm; (x) liability to execution; and (xi) the incident of residuarity. Honore conceded that while not all of these incidents are present in all cases in which we speak of property, yet they

represent the paradigm of full ownership, against which various types of incomplete or partial ownership must be understood. Honore thus elaborates not only the kind of *rights* we have when we own, but also further incidents, or features of ownership, including duties and liabilities, which provide a more accurate picture. Properly understood then, "property is a bundle of rights" expresses the thesis that property constitutes a legal complex of various normative relations, not simply rights.

The bundle of rights theory conceives of proprietary rights as a bundle held by the property owner against the rest of the world. This bundle also contains duties and liabilities. The bundle of rights theory is the dominant paradigm applied by Western legal philosophers, combining the theories of Wesley Hohfeld and Anthony Honore. Hohfeld developed the theory that property rights are rights between people, rather than rights in relation to things. According to him, the difference between personal and proprietary rights is that proprietary rights can be enforced as against the rest of the world, whereas personal rights can only be enforced against those who are parties to the agreement. Honore gives a list of rights and the ensuing duties and liabilities that proprietary rights ordinarily entail. He extends Hohfeld's theory, applying it to things themselves.

Despite the fact that the bundle of rights theory is the pre-eminent Western jurisprudential theory of property, it has been profoundly criticized by a number of different theorists. Generally, these criticisms centre on the fact that the bundle of rights theory does not adequately explain the right to property (Penner).[iv]

Property can be identified by those rights which attend it. But, by looking at what rights attend a thing, the rights to it can be categorized as proprietary. Thus, as an analytical tool, the bundle of rights theory possesses an inherent problem. To a very large extent, the bundle of rights theory diluted property of any substantive meaning it may have acquired in legal discourses. Whereas even Blackstone had emphasized on the element of excludability, the bundle metaphor merely recognized the "right to exclude" as one among several rights and privileges accorded by the legal system to an owner. The bundle of rights concept however proved to be of significance in functional terms, primarily in determining whether something had been removed from the bundle and was therefore short of full-property; but it could never answer what full property was, at any given point of time.

The essence of the interjection of the discourse on cybersquatting and other infringements of domain names must not be lost. My argument here will be twofold. First, I will look at the use of the bundle of rights theory in the area of domain name dispute resolution, particularly as relates to cybersquatters and typosquatters. It will be my contention that the bundle of rights theory adequately explains the phenomenon of proprietary rights vested in original owners of trademarks and names. However, the theory has not been emphatically engaged by courts and juridical bodies because of a lack of any adequate juristic mechanism with which to analyze property rights and the incidents of ownership. Second, I will argue that the bundle of rights theory is a particularly appropriate mode of analysis in respect of proprietary interests in infringed domain names because of the special nature of trademarks. The determination of the theory that should be used to analyze domain name titles requires very much a policy decision by the courts. This decision is important, because it ultimately affects the substantive rights of all parties. I shall come to this under the fifth segment of this paper.

## 3. A COMPARATIVE OVERVIEW OF JURIDICAL RESPONSES

Even though the internet had not been designed to be a subject of private property rights, the exponential growth of its popularity and usage has made it inevitable for the lawyers and law courts to get involved with its processes. In the absence of any other alternative, matters pertaining to the infringement of internet-related rights have been addressed through the mechanisms of property law (Balganesh 2006). With regard to the phenomena of cybersquatting and typosquatting, the approach of juridical bodies across the world has been to apply conventional property law and/or more recent intellectual property laws relating to trademarks and copyright to claims brought by claimants

(Chalikian 2001; Holland 2005).

### 3.1 United States

Since the United States continues to play a leading role in the development of legal approaches to internet-related problems, it would serve the ends of this paper to consider the attitude of its legal system to the phenomena of cybersquatting and typosquatting. In the mid-1990s, trademark owners wishing to bring suit for infringement filed their claims under either the Lanham Act,[v] or the Federal Trademark Dilution Act (FTDA).[vi] Traditional actions for domain name disputes therefore fell under three categories, namely, trademark infringement; confusion of source infringement; and dilution of a famous mark (Mercer 2000).

The two decisions most clearly demonstrating the readiness of the law courts to apply their understanding of traditional trademark law to cybersquatting involved one Dennis Toeppen. In *Panavision International v. Toeppen*,[vii] Toeppen had reserved panavision.com as a domain name and demanded US$13,000 from Panavision Corporation to discontinue its use. Toeppen had also reserved domain names consisting of the trademarks of other large companies. Following a suit instituted by Panavision, the court granted summary judgment in favor of Panavision, declaring that Toeppen's conduct constituted commercial use of Panavision's trademark and thus violated trademark laws. The appellate court upheld the decision. Similarly in *Intermatic Inc. v. Toeppen*,[viii] Toeppen had reserved the domain name intermatic.com whereas Intermatic Inc. had an incontestable federal registration for its "Intermatic" mark and prior to reserving the intermatic.com domain name, Toeppen had never used the term "intermatic" for any purpose. When Intermatic Inc. became aware that Toeppen had reserved the mark intermatic.com as a domain name, the company demanded that Toeppen relinquish or assign the intermatic.com domain name and discontinue its use. Toeppen refused. The court upheld Intermatic's trademark infringement claim and upheld, finding that Toeppen had made commercial use of the domain name.

As a result of the criticisms against the potency of the Lanham Act and the FTDA to effectively tackle cybersquatting despite the above two cases, the US Congress passed the Anti-Cybersquatting Consumers Protection Act (ACCPA) in November of 1999.[ix] The ACCPA provides a specific cause of action for cybersquatting, incorporating provisions of the existing framework of trademark infringement and trademark dilution laws. Accordingly, traditional trademark principles are modified and expanded in order to apply trademark law to Internet-specific problems. ACCPA attempts to prevent cybersquatting by creating a private cause of action by the owner of a trademark or a personal name, against any person who: (i) has a bad faith intent to profit from the mark, including a personal name which is protected as a mark under this section; and (ii) registers, traffics in, or uses a domain name that -

(a) in the case of a mark that is distinctive at the time of registration of the domain name, identical or confusingly similar to that mark;

(b) in the case of a famous mark that is famous at the time of registration of the domain name, identical or confusingly similar to or dilutive of such mark.[x]

The ACCPA's definition of cybersquatting, as it relates to trademarks, creates two different standards: one for distinctive marks, and another, more protective standard for famous marks. Protection by the statute is triggered when the trademark in question is either distinctive, famous, or both at the time the defendant registered the domain name, thereby providing protection for non-famous marks. "Famous" and "distinctive" are not defined within the ACCPA itself. The term "distinctive" is a term of art within trademark law, referring to the degree of uniqueness that a trademark possesses. The relative distinctiveness of a trademark determines the degree of protection it can receive. The term "famous" is also not defined within the ACCPA. The ACCPA's use of famousness as a factor in determining trademark protection is similar to its use in the Federal Trademark Dilution Act, where it is defined. Another significant part of the ACCPA is the element of "bad faith" in the registration of a domain

name.[xi] The Act provides the courts with nine factors to help guide their determination of bad-faith. However, these factors are guidelines, not an all-inclusive list of factors to be used by the courts. The ACCPA makes it flexible for the courts to consider factors beyond those enumerated. An injunction, damages and transfer, forfeiture, or cancellation of the domain name are available under ACCPA.[xii] Under the ACCPA, therefore, a cause of action for cybersquatting lies where: (1) plaintiff's mark is "distinctive" or "famous" at the time of registration of the domain name; (2) the cybersquatter's domain name is (a) identical or confusingly similar to a distinctive mark, or (b) identical, confusingly similar to, or dilutive of a famous mark; *and* (3) the cybersquatter acted with a "bad faith intent to profit" from the mark. What is most striking about this statute is that it does not condition a cause of action on trademark infringement or dilution; it is enough that the domain name be identical or confusingly similar in appearance to a distinctive trademark. Further, unlike the FTDA, the ACCPA does not require that a mark be famous to receive protection against dilution. No less important, the ACCPA does *not* require formal commercial use of the trademark-domain name, but instead targets cybersquatters who merely register domain names, as well as cybersquatters who traffic in (i.e., sell, purchase, loan, pledge, license) or otherwise use domain names. By proscribing the bad faith registration of domain names, the ACCPA prevents cybersquatters from exploiting the settlement value of cases against trademark holders wishing to avoid the expense of litigation.

The numerous cases decided by US courts under the ACCPA since 1999 have been subject of rigorous scholarly analysis and need not be revisited here.[xiii] However, one case that would accentuate the thrust of this paper is *Shields v. Zuccarini*. Here, the plaintiff, Joseph Shields, worked as a graphic artist who designed, exhibited, licensed, and marketed the Joe Cartoon animated creature for more than fifteen years. In June 1997, Shields created a website with the registered domain name Joecartoon.com. In November 1999, Zuccarini registered five variations of Shields's original website. These sites included: joescartoon.com, joecartoon.com, joescartons.com, joescartoons.com, and cartoonjoe.com. Upon reaching Zuccarini's site, visitors were "mousetrapped" and needed to click on various advertisements to exit the site.

In its analysis, the court applied the three factors needed to succeed on an ACCPA claim - whether the mark was famous or distinctive at the time of registration, whether the domain name is "identical or confusingly similar to" the mark, and whether the domain-name registrant acted in bad faith. The court found Joe Cartoon to be "distinctive and famous" as a mark. Furthermore, the domain names were "identical and confusingly similar" enough to the Joecartoon.com website that Internet users would be confused by Zuccarini's site. Finally, the court found that Zuccarini acted in bad-faith and with intent to commercially exploit Shields's protected mark, and thus, found in favor of Shields. Holding that typosquatting is a violation of the federal law against cybersquatting, Shields illustrates the Third Circuit's willingness to broaden the scope of the ACCPA beyond the plain language in order to better fulfill the Act's explicit goals.

### 3.2 United Kingdom

Courts in the United Kingdom (UK) have taken the cybersquatting issue a step further than United States courts. In July 1998, the Court of Appeal held in *British Telecommunications Plc & Ors v. One in a Million Ltd & Ors*,[xiv] that the practice of registering famous brand names as Internet domain names without consent is illegal because such registrations amounted to passing off and instruments of fraud. In that case, a company called One in a Million, and other related defendants, registered a number of domain names in both the .com and .uk TLDs in the hope of selling them. The court reasoned the registration of these domain names amounted to false representations that they were associated with the brand owners. Anyone conducting a "who is" search on one of these domain names, for example, would find that the registrant was One in a Million, Ltd. and a substantial number of people would thus conclude this company was somehow associated with the trademark owner, which would amount to passing off. Like the U.S. courts, the UK court found that, even though there was no active website, reserving the domain in order to sell it was use in the course of trade. This case

was not decided under U.S. trademark dilution law, and therefore was not limited by the Lanham legal requirement that the mark be "famous." The holding could also apply to the reservation of non-famous marks in the UK.

### 3.3 Thailand

The phenomenon of cybersquatting was unheard of in Thailand until May 2000 when the first domain name took place (Ratanayu 2002). In *James H.W. Thompson Foundation and The Thai Silk Company Limited v. Panarach Puangpetch,*[xv] the James H.W. Thompson Foundation, owner of the famous trade name Jim Thompson House, and its affiliate, the Thai Silk Co., Ltd., owner of the trademark Jim Thompson, filed a complaint with the World Intellectual Property Organization (WIPO) Administrative Panel on May 16, 2000, asking for the transfer of the domain names jimthompsonhouse.com and jim thompsonhouse.org from a Thai citizen who had registered them to the James H.W. Thompson Foundation. The Panel ruled in favor of the complainants, stating that the grounds for the complaint were compelling under the UDRP. In accordance with UDRP, the Administrative Panel found (i) that the disputed domain names are identical or confusingly similar to the complainant's trademark; (ii) that the respondent had no right or legitimate interest in the domain names; and (iii) that the domain names were registered and being used in bad faith. The Administrative Panel ordered the transfer of the domain names to the complainants.

### 3.4 Japan

In Japan, the *JACC Company's Case*[xvi] marked the beginning of litigation with regard to cybersquatting (Yonehara 2003). Here, a renowned Japanese credit card company and owner of the "JACCS" trademark, sued the defendant, a portable toilet manufacturer, cellular phone distributor, and owner of the "jaccs.co.jp" domain name. JACCS claimed that the "JACCS" name was well-known in Japan and that Nihonkai Pakuto's registration of the "jaccs.co.jp" name represented a misappellation of source under the law. The district court held that the defendant's use of the "jaccs.co.jp" name was a violation of the UCPL. The court extensively noted that the defendant's attempt to distinguish "JACCS" and "jaccs.co.jp" between the lower case and upper case spellings was immaterial, because a typical Internet user would nonetheless be confused. On appeal, the Nagoya High Court upheld the Toyama District Court ruling. Here, the court refused to make the distinction between the plaintiff's all capital letters usage of the "JACCS" name and the defendant's all lower case usage in "jaccs.co.jp." In February 2002, the Japan Supreme Court rejected the defendant's appeal, preserving the lower court's decision. While Japan had initially shown a lackadaisical attitude towards vigorous legal action against cybersquatting, it is remarkable to note that the Japanese government had initiated the law that amended the Unfair Competition Prevention Law ("UCPL") to specifically prohibit cybersquatting and thus protect trademark holder's rights to domain names (Yonehara 2003).[xvii]

### 3.5 South Africa

Although by virtue of its legal tradition, South Africa belongs to that category of states where disputes about domain names were initially subject to the jurisdiction of the regular courts. While the jurisdiction of the ordinary courts has not been ousted, the preferred forum for complaints against alleged domain name infringements is the procedure afforded by the UDRP established pursuant to the new-fangled Alternative Dispute Resolution Regulations, 2006.[xviii] For more than a decade, the South African Institute of Intellectual Property Law (SAIIPL) has been the vanguard in the anti-cybersquatting and anti-typosquatting campaign in South Africa, fully committed to the drafting of the ADR Regulations and in dealing with all disputes relating to domain names (Alberts 2007). After a long period of delay and debates, the administration and control of the .za domain was removed from the South African Department of Commerce and vested in an independent private organization (Greenberg 2004).

Notwithstanding the criticisms leveled against the .za ADR, Pistorius (2008) has commended the procedure as "an efficient alternative to court litigation." Some of the decisions emanating from this

procedure have been quite significant as the procedure consistently engages the application of traditional trademark precepts in addressing the phenomena of cybersquatting and typosquatting (Alberts 2007; Pistorius 2008).

In *Mr. Plastic Mining and Promotional Goods v. Mr. Plastic CC,*[xix] where the complainant claimed rights over the use of an unregistered trade mark "Mr. Plastic", which another party had registered as domain name, the adjudicator rejected the claim, recognizing that there was concurrent use of the name – an unequivocal pointer to the relevance of Anglo-American legal thinking on the concept of property.

In *Telkom SA Limited v. Customer Care Solutions (Pty) Ltd,*[xx] the registrant registered telkombusiness.za; telkom-business.co.za; telkom-internet.co.za; telkomcorporate.co.za; telkom-corporate.co.za in respect of its services which the complainant claimed were abusive of its trademark rights at common law. Upholding the contention of the complainant, the adjudicator ordered that the domain names be transferred to the Complainant.

Another decision that will strengthen the pivot of this paper was that in *Standard Bank of South Africa Ltd v. Daniel Cox,*[xxi] where the registrant had registered standerdbank.co.za, standarbank.co.za, wwwstandardbank.co.za, standerdank.co.za, standardank.co.za, stanardbank.co.za, standardban.co.za, standadbank.co.za, standardbak.co.za, stndardbank.co.za, stadardbank.co.za, and sandardbank.co.za as domain name without having any legal interest in the business of Standard Bank, the complainant. The adjudicator held that all those domain names were identical to the Complainant's STANDARD BANK trade mark and thus infringed the complainant's rights. The domain names were ordered transferred to the complainant. This decision had established the precedent in South Africa that typosquatting is unlawful.

The obvious conclusion from the discussion in this segment is that while the outcomes of domain name complaints have not been uniform, a common thread of reasoning is dominant, namely, the interpretation of domain name rights in the language of property. This has been applied in the classic sense of cybersquatting, especially where the domain name holder attempted to sell the name to the trademark holder, e.g., VW, in *Virtual Works, Inc. v. Volkswagen of America, Inc.*; *JACC's Case*, etc When there was no bad faith intent to profit found, however, the domain name was not transferred, even though there had been prior trademark infringement, as seen in *Interstellar Starship Services, Ltd. v. Epix, Inc.*; Mr Plastic, etc The ACCPA has also been applied when the bad faith intent to profit comes not from selling the domain name back to the trademark holder, but from selling advertising seen by those accidentally hitting the site, as seen in *Shields v. Zuccarini* and *JACC Company's Case*.

Although many commentators say that trademark law has proven to be inadequate in the Internet arena for providing a remedy for trademark owners, courts have continued to apply trademark and proprietary laws to provide assistance to trademark holders, even if they are inadequate and ineffective judicial remedies. This uncertainty regarding the applicability of trademark laws to the Internet has produced inconsistent judicial decisions and created extensive monitoring obligations, unnecessary legal costs, and uncertainty for consumers and trademark owners alike (Mercer 2000; Gilwit 2003; Holland 2005).

The issues coming out of this expansion of trademark holder rights in the context of domain name disputes are whether and to what extent these additional rights can be squared with the foundational principles upon which they were constructed. That foundation rests upon two pillars. The first is a product of practical concerns and competing interests which were found to justify the alteration of certain tenets of trademark protection for the purpose of addressing the very specific and perceptually grave harm of cybersquatting. The second is composed of theoretical justifications for the expansion of trademark protections toward a private property-like conception of broad exclusive rights, but limited by basic constitutional interests. I shall elucidate on these issues shortly.

## 4. DOMAIN NAMES AS *RES*: RETURN TO THE BASICS

It is of utmost importance for trademark owners to use their trademarks as domain names. If an Internet user does not know the domain name of a company, the user may conduct a search on the Internet for the company's trademark. To ensure that a user gets to their site easily, it is to the benefit of the company to use its trademark as a domain name. In turn, when a company cannot use its trademark as a domain name because another Internet user registered the name first, the trademark owner's ability to profit from their mark decreases.

Associating domain names with the law of property is attractive for many reasons. The right to a domain name is the right to control the social and economic agenda of an abstract entity, which implies its separation from a community of similar entities, from the public domain. In trademark law, as in property, people are concerned with acquiring possessions and protecting 'mine' against 'yours', preserving the right holder's exclusive possessions from trespassers. Like private property, to have a trademark is to have an exclusive title, which confers on its owner the right to use, the right to exclude all others both from use and possession, and the right to transmit use and possession to others (Zemmer 2007). It means that a private individual has the right to determine what will be done with an object. It embraces what is not common to all, but controlled by a lesser number of people, whether one individual or more.

The trespassory rules of property law provide the great advantage of legally enforceable physical and intangible boundaries. They are a powerful economic tool and provide the connection between rights and rewards. Rules of trespass enforce the owner's strong right to exclude, which is complemented by, for example, the rules of contract law and conveyancing, which also safeguard the owner's right to transfer an object. The same applies to intellectual property. According to Harris (1996: 44), "By instituting trespassory rules whose content restricts uses of the ideational entity, intellectual property law preserves to an individual or group of individuals an open-ended set of use-privileges and powers of control and transmission characteristic of ownership interests over tangible items."

As a property right, a trademark creates a relational right. It is not a right between a person and an object but a right between people with respect to objects. It follows that a trademark domain name, like property, is a matter of rights. The right itself is intangible, even where the object is tangible. Individuals tend to lose track of the distinction between the physical relation between a person and an object and between the normative - moral or legal - nature of property that determines relationships between persons with respect to things, because the two concepts are frequently conflated in everyday life.

Consequently, we can identify two different, but complementary, senses of property. First, property as a set of legal relations. Second, in the conversational sense, property as a thing, a *res*, which usually implies an owner.

Trademarks secure a bundle of rights for right holders that, singly or collectively, define the relationship of an owner to a resource and between the owner and other individuals (Gray 1991). Ownership has variously been defined as an "abstract bundle of legal relations", "a cluster-right", "a complex aggregate of rights", "a range of ownership interests along the ownership spectrum", "complexes", or a synonym for "bundle of sticks" (Zemmer 2007: 62).

There is no requirement that property be fixed in a tangible medium, and thus a person can have property rights in tangible or intangible objects. Owners of tangible property have the right to exclusive possession of that property, granting the owner the right to prevent others from taking possession of it. Owners of intangible property have identical rights, including the unrestricted right to use and possess the property, as well as the right to exclude all people from their property, even though it is not in a fixed and tangible medium. After all, as in Heller's words "private property can be defined in terms of a core bundle of rights chosen from the infinite relations that may exist among people with respect to a scarce resource" (Heller 1998: 665).

The point must therefore never be lost on scholars and jurists that the primary right conception of exclusion, much like the primary right conception of contractual performance, derives its normative content from an underlying moral ideal on which the institution of property bases itself: inviolability (Balganesh 2008). Inviolability represents a principle central to peaceful coordinated social existence, and the right to exclude, as a correlative to the duties that derive from it, converts it into a legal (as opposed to moral) norm. The right to exclude, therefore, remains the defining ideal of property. If the idea of property is understood outside of its remedial context, and instead is viewed as a social institution that coordinates access to and use of scarce resources, the primary or correlative right conception begins to make logical sense. Recasting the right to exclude along these lines, it is hoped, will contribute towards moving property debates away from their singular emphasis on remedialism and towards a broader analytical framework for the institution.

Corporations, like individuals, have an identity with which people associate. They have property rights in their identities, entitling them to exclude and prevent others from exploiting their identity. Because domain names constitute part of corporations' and individuals' identities, they assume the same property rights in the domain name itself, the right to exclude and prevent others from exploiting their domain name (Gatsik 2001). Therefore, when cybersquatters and typosquatters victimize corporations and individuals, they infringe upon the latter's property interest in their identities. This is the trend of the juridical decisions from all over the world and despite all the vitriolic criticisms, it is worthy of acceptance.

## 5. THE BUNDLE OF RIGHTS THEORY: A PREVENTIVE THERAPY AGAINST CYBERSQUATTING

The primary reason trademarks and domain names come into conflict is that they are both used to identify individuals, companies, or other entities. The Internet has engendered substantial debate about whether domain names are a new type of intellectual property that can be obtained, sold, transferred and encumbered. Domain names are intriguing and controversial, because they are significant for economic reasons. With the globalization and commercialization of the Internet, domain names have taken on a new significance as business addresses. The identity of many businesses on the Internet is solidly associated with their domain names. As the commercial use of the Internet has expanded, companies, entrepreneurs, and other who also want a presence on the Internet want domain names that are easily associated with their company (or personal) name or product. As a consequence, domain names have emerged as a commercial property right overlapping, but remaining distinct from, trademarks, trade names, and corporate names.

Based on all the totality of decisions considered in this paper and elsewhere, it is not difficult to discern that the protection of legitimate expectations and the rejection of fraud were dominant themes in the minds of adjudicators of domain name disputes in diverse jurisdictions. Although the interventionist posture of regular courts in domain name infringement disputes was a rather *ad hoc* incidence as evident in their initial focus on intellectual law framework, one might be safe to posit that there could not have been a better approach to the phenomena of cybersquatting and typosquatting in the era before statutory interventions against the phenomenona (Manta 2009).

Why is the location of this discourse within the law of property necessary any way? Locating the struggle against cybersquatting and typosquatting within the framework of property law is an important pathway for human understanding and organizing new information. It also serves rule of law imperatives. Well-ordered legal systems should be based on normative principles that ensure against arbitrary power and guide conduct in a manner that is clear and consistent as well as fair. Absent clarity and competency, expectations are frustrated and public and private affairs become more difficult to accomplish. Classifying domain names as property has tremendous legal consequences under the fundamental laws of various countries (Chaudri 2006).

Beyond constitutional implications, additional legal consequences flow from classification of domain

names as property. It is determinative of issues ranging from the ability to prevent trespass, conversion, or nuisance under the common law, to mortgage the domain name in question, to freely convey it or split it between present and future interests, to receive special treatment under state laws, and to impose or avoid trade constraints.

Another important aspect is that conceiving domain names as property allows for an *in rem* action against the domain name should the complainant be unable to locate or obtain personal jurisdiction over the domain name holder.

Intellectual property laws, and invariably, proprietary rights embedded in them assist the courts in balancing the interests of competing parties. If nothing more, the interjection of intellectual property law in the novel developments ensured that the notion of the right to exclude would become the defining compass for the protection of trademark owners against unscrupulous domain name registrants.

Of course, those who are given the right to exclude others from a valued resource typically also are given other rights with respect to the resource - such as the rights to consume it, to transfigure it, to transfer it, to bequeath or devise it, to pledge it as collateral, to subdivide it into smaller interests, and so forth. These other rights are obviously valuable and important, and it is not improper to speak of them as part of the standard package of legal rights enjoyed by property owners in most contexts. My claim is simply that in demarcating the line between 'property' and 'non-property' - or 'unowned things' (like the air in the upper atmosphere or the resources of the ocean beyond a certain distance from shore) - the right to exclude others is a necessary and sufficient condition of identifying the existence of property (Zellmer and Harder 2008). Whatever other sticks may exist in a property owner's bundle of rights in any given context, these other rights are purely contingent in terms of whether we speak of the bundle as property. The right to exclude is in this sense fundamental to the concept of property (Mossoff 2003).

To regard a trademark as property is important, because then it must be protected no matter where it is infringed. Arguably, that protection should extend to any forum. It should make no difference in what forum or setting a trademark is infringed, whether in Johannesburg, Mumbai, or cyberspace. A commercial entity's reputation can just as easily be damaged on the Internet as in any other situation. As we have seen, nearly all trademark and domain name disputes involve someone using another person's name, company name, or trademark as a domain name, usually for their own gain. These individuals have come to be known as cybersquatters and typosquatters.

Since it is largely settled that trademarks create property rights (Johnson 2001; Manta 2009), the right to a trademark can therefore not be one in gross, and cannot exist as a mere abstract right, independent of or disconnected from all settings in which they are used. The right to a domain name, therefore, where appurtenant to a trademark, becomes a property right as soon as it identifies the trade. Viewing trademark domain names this way, just as various juridical bodies around the world have viewed it, would justify the submission that the rights of an owner of a trademark that appears on the World Wide Web as a domain name are inseverable and inseparable from the bundle of proprietary rights held by that owner.

If the thesis in this paper is followed, the right of any registered trademark owner to the use of his/her trademark as domain name would be preserved and no matter how ingenious adventurous cybersquatters and typosquatters may become, there would have been an established expectation that any reconfiguration, misspelling of the trademark would warrant a forfeiture to the trademark owner.

## 6. CONCLUSION

This paper recognizes the phenomena of cybersquatting and typosquatting as a problem that exists because of the Internet, and which is likely to continue into the future with the increased use and ease of Internet access and decreased costs of domain name registration. No doubt, Internet domain names

serve as valuable assets to businesses or individuals because they allow consumers to identify their presence on the web. Because of the value associated with domain names, cybersquatters often attempt to sell the domain name to the trademark holder or famous person, use the domain name to compete against the trademark holder's existing business, or perpetuate fraud upon consumers. Cybersquatters and typosquatters typically victimize business entities or famous people because the domain name has monetary value, regardless of whether the cybersquatter attempts to sell the domain name to the business or entity or traffics in consumers on the Internet.

This paper contributes a voice to the philosophical thinking that inevitably underpins the innovative attitude of law courts and other quasi-judicial bodies dealing with domain name disputes. An attempt has been made to accentuate the location of domain name disputes and the incidence of cybersquatting within the realm of property law. Property gives a person, the owner of a thing, legal rights to control that thing and to exclude all the world not just specified individuals but a large class of others from possession or use of that thing. People tend to feel strong attachments to things known as property. Land and certain types of personal property form important components of a person's identity and self-actualization. The same applies to trademark-domain names.

While this paper makes no pretension about the foreseeable resistance to its thesis, consistent efforts of the courts in protecting and preserving the real and collateral rights of trademark owners in the exclusive use of their trademarks as domain names is a reaffirmation of the relevance of the bundle of rights theory as well as its currency.

Far from being an *ex cathedra* pronouncement on all the dynamics that would inform the formulation of a coherent philosophical foundation for the judicial assertiveness against cybersquatting and typosquatting, this paper would have served its purpose if it stimulates further intellectual engagement.

**ACKNOWLEDGEMENTS**

I wish to acknowledge the efforts of every one involved in organizing the South African Cyberlaw and ICT Conference held in Johannesburg, 22-24 July 2009, and in particular, Mr. Sizwe Snail, for his unfailing warmth and encouragement.

**ABOUT THE AUTHOR**

LL.B (Honours), LL.M, Obafemi Awolowo University, Ile-Ife, Nigeria; LL.M Human Rights & Democratisation in Africa, University of Pretoria, Pretoria, South Africa; PG Dip. International Human Rights, Åbo Akademi University, Turku, Finland; JSD *cum laude*, University of Notre Dame, Notre Dame, Indiana, USA; Barrister & Solicitor (Nigeria). Main teaching and research interests: Public International Law, Legal Theory, Human Rights, and Comparative Constitutionalism. Professor of Law at the Walter Sisulu University School of Law, South Africa. The South African National Research Foundation (NRF) currently rates Professor Olowu as an "Established Researcher" for his work across various disciplines.

## REFERENCES

**Books**

Blackstone, W. (1765-1769), Commentaries on the Laws of England 2, Clarendon Press, Oxford.

Harris, J.W. (1996), Property and Justice, Oxford University Press, Oxford.

Hohfeld, W. (1923), Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays, Walter Wheeler, Cook-New Haven.

Van der Merwe, D. (2000), Computers and the Law, Second edition, Juta & Co., Kenwyn.

**Chapters in Books**

Greenberg, D.J. (2004), 'Trademarks, Domain Names and Meta Tags', in Cyberlaw: The of the Internet in South Africa, eds. R. Buys and F. Cronje, Van Schaik, Durban.

Honore, A. (1961), 'Ownership' in Anthony Guest (ed), Oxford Essays in Jurisprudence: A Collaborative Work, Oxford University Press, Oxford.

**Journals**

Alberts, W. (2007), "The New Domain Name Dispute Resolution Structure", The Quarterly Law Review for People in Business, 15: 66.

Balganesh, S. (2006), "Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass", Michigan Telecommunications and Technology Law Review, 12: 265.

Balganesh, S. (2006), "Demystifying the Right to Exclude: Of Property, Inviolability, and Automatic Injunctions", Harvard Journal of Law and Public Policy, 31: 593.

Belczyk, T. (2002), "Domain Names: The Special Case of Personal Names", Boston University Law Review, 82: 485.

Chalikian, A. (2001), "Cybersquatting", Journal of Legal Advocacy and Practice, 3: 106.

Chaudri, A. (2007), "Internet Domain Names and the Interaction with Intellectual Property", 23 Computer Law and Security Report, 62.

Cotton, B.B. (2002), "Prospecting or Cybersquatting: Registering Your Name Before Someone Else Does", John Marshall Law Review, 35: 287.

Efroni, Z. (2003), "The Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy: New Opportunities For International Forum Shopping?", 26 Columbia Journal of Law and Arts, 26: 335.

Gatsik, J.H. (2001), "Cybersquatting: Identity Theft in Disguise", Suffolk University Law Review, 35: 277.

Gilwit, D.B., (2003), "The Latest Cybersquatting Trend: Typosquatters, Their Changing Tactics, and How To Prevent Public Deception and Trademark Infringement", Washington University Journal of Law and Policy, 11: 267.

Gole, R.W. (1999), "Playing the Name Game: A Glimpse at the Future of the Internet Domain Name System", Federal Commercial Law Journal, 51: 403.

Golinveaux, J. (1999), "What's in a Domain Name: Is "Cybersquatting" Trademark Dilution?", University of San Francisco Law Review, 33: 641.

Graham, J. et al (2001) "Cybersquatting: The Latest Challenge in Federal Trademark Protection" Duke Law and Technology Review, 9.

Gray, K. (1991), "Property in Thin Air", Cambridge Law Journal, 50: 252.

Gusewelle, D.A. (2004), "Typosquatters, The Tactical Fight Being Waged by Corporations, and Congress' Attempt to Fight Back in the Criminal Arena: U.S. v. Zuccarini", Vanderbilt Journal of Entertainment Law and Practice, 7: 146.

Hale, P.W. (2001), "The Anticybersquatting Consumer Protection Act & Sporty's Farm L.L.C. v. Sportsman's Market, Inc.", Berkeley Technology Law Journal, 16: 205.

Heller, M. (1998), "The Tragedy of the Anticommons: Property in the Transition from Marx to Markets", Harvard Law Review, 111: 621.

Hohfeld, W.N. (1913-14), "Some Fundamental Legal Conceptions as Applied in Judicial Reasoning", Yale Law Journal, 23: 16.

Hohfeld, W.N. (1916-17), "Fundamental Legal Conceptions as Applied in Judicial Reasoning", Yale Law Journal, 26: 710.

Holland, H.B. (2005), "Tempest in a Teapot or Tidal Wave? Cybersquatting Rights and Remedies Run Amok", Journal of Technology Law and Policy, 10: 301.

Johnson, S.J. (2001), "Internet Domain Name and Trademark Disputes: Shifting Paradigms in Intellectual Property", Arizona Law Review, 43: 465.

Jones, G.R. (2007), "What's In A Name? Trademark Infringements In Cyberspace", The Alabama Lawyer, 68: 70.

Lipton, J.D. (2005), "Beyond Cybersquatting: Taking Domain Name Disputes Past Trademark Policy", Wake Forest Law Review, 40: 1361.

Litman, J. (2000), "The DNS Wars: Trademarks and the Internet Domain Name System", Journal of Small and Emerging Business Law, 4: 149.

Manta, I.D. (2009), "Privatizing Trademarks", Arizona Law Review 51: 381.

Marsh, T. (2002), "Shields v. Zuccarini: The Role of the Anticybersquatting Consumer Protection Act in Fighting Typosquatting", Toledo Law Review, 33: 683.

Mercer, J.D. (2000), "Cybersquatting: Blackmail on the Information Superhighway", Boston University Journal of Science and Technology, 6: 11.

Merrill, T.W. (1998), "Property and the Right to Exclude", Nebraska Law Review, 77: 730.

Mossoff, A. (2003), "What Is Property? Putting the Pieces Back Together", Arizona Law Review, 43: 371.

Mota, S.A. (2003) "The Anticybersquatting Consumer Protection Act: An Analysis of the Decisions from the Courts of Appeals", John Marshall Journal of Computer and Information Law 21: 355.

Penner, J. (1996), "The 'Bundle of Rights' Picture of Property", UCLA Law Review, 43: 711.

Pistorius, T. (2008), ".za Alternative Dispute Resolution Regulations: The First Few SAIIPL Decisions", Journal of Information, Law and Technology, 2 [Online Journal].

Ratanayu, A. (2002) "Cybersquatting in Thailand: The Thai Trademark Act and the Uniform Domain Name Dispute Resolution Policy" Buffalo Intellectual Property Law Journal, 1: 203.

Strahilevitz, L.J. (2006), "Information Asymmetries and the Rights to Exclude", Michigan Law Review, 104: 1835.

Woollacott, C.A.R. (2000), "Name Dropping: Recent Anti-cybersquatting Legislation Offers Some Relief to Trademark Holders", 23 Los Angeles Lawyer, 23: 28.

Yonehara, B.T. (2003), "Landoftherisingsun.Co.Jp: A Review Of Japan's Protection Of Domain Names Against Cybersquatting", IDEA: The Journal of Law and Technology, 43: 207.

Zellmer, S.B. and Harder, J. (2008), "Unbundling Property in Water", 59 Alabama Law Review, 679.

Zemmer, L. (2007), "What Copyright Is: Time to Remember the Basics", Buffalo Intellectual Property Law Journal, 4: 54.

**Websites**

Internet Corporation for Assigned Names and Numbers ("ICANN"), Rules for Uniform Domain Name Dispute Resolution Policy, at http://www.icann.org/udrp/udrp-policy-24oct99.htm (accessed 06 July 2009).

**END NOTES**

[i] See Internet Corporation for Assigned Names and Numbers ("ICANN"), Rules for Uniform Domain Name Dispute Resolution Policy (also known as the "Rules of Procedure"), at http://www.icann.org/udrp/udrp-policy-24oct99.htm (accessed 06 July 2009).

[ii] 15 U.S.C. § 1125.

[iii] See *Electronics Boutique Holding Corp. v. Zuccarini*, 56 U.S.P.Q. 2d 1705 (E.D. Pa. 2000); *Shields v. Zuccarini*, 89 F. Supp. 2d 634, affirmed 254 F.3d 476 (3d Cir. 2001).

[iv] See also Sackville J in *Wily v St George Partnership Banking Ltd*, observing that one of the problems attending analysis of proprietary rights is a 'chicken and egg problem' of circularity of definition.

[v] 15 U.S.C. 1051-1127 (Supp. 2001).

[vi] FTDA, Pub. L. No. 104-98, 109 Stat. 985. Amended by ***Federal Trademark Dilution Act*** of 2006.

[vii] *Panavision International v. Toeppen*, 945 F. Supp. 1296, 1299 (C.D. Cal. 1996).

[viii] *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227, 1230 (N.D. Ill. 1996).

[ix] Act 15 U.S.C. 1125.

[x] Anticybersquatting Consumer Protection Act 15 U.S.C. 1125(d)(1)(A).

[xi] Anticybersquatting Consumer Protection Act 15 U.S.C. 1125 (c)(1) (Supp. III 1997).

[xii] Id.

[xiii] See, for example, Carrol, L. (2000), "A Better Way to Skin the Cat: Resolving Domain Name Disputes Using State Unfair Competition Law", American Bar Association Section of Intellectual Property Law Newsletter; Graham, J. et al (2001) "Cybersquatting: The Latest Challenge in Federal Trademark Protection" Duke Law and Technology Review 9; and Mota, S.A. (2003) "The Anticybersquatting Consumer Protection Act: An Analysis of the Decisions from the Courts of Appeals", John Marshall Journal of Computer and Information Law 21: 355, discussing cases such as *Northern Light Technology, Inc. v. Northern Lights Club*, 97 F. Supp. 2d 96, 100-01 (D. Mass. 2000); *Sporty's Farm LLC v. Sportsman's Marketing Inc.*, 202 F.3d 489, 497 (2d Cir. 2000); *Virtual Works, Inc. v. Volkswagen of America, Inc.*, 238 F.3d 264, 271 (4th Cir. 2001); and *People for the Ethical Treatment of Animals v. Doughney*, 263 F.3d 359 (4th Cir. 2001), among others.

[xiv] Appeal No. 98/0092-95B, Court of Appeal, 23 July 1998.

[xv] WIPO Case No. D2000-0436.

[xvi] *Kabushiki Kaisha JACCS Co., Ltd. v. Yugen Kaisha Nihonkai Pakuto*, Toyama Dist. Ct. (Dec. 12, 2000). See also *Sankyo Co., Ltd. v. Zhu Jiajun*, WIPO UDRP Administrative Panel, Case No. D2000-1791 (Mar. 23, 2001).

[xvii] Fusei Kyoso Boshi-ho [Unfair Competition Prevention Law], Law No. 14 of 1934, amended, Law No. 47 of 1993, art. 2.

[xviii] Issued pursuant to the Electronic Communications and Transactions Act 25 of 2002 ('the Act') and published on 22 November 2006 (GN R1166 Government Gazette 29405 (Reg Gaz 8587), available at <http://www.domaindisputes.co.za>.

[xix] ZA2007-0001.

[xx] ZA2007-0004.

[xxi] ZA2007-0006 (02 November 2007).

# Sexual Exploitation in the Online World - a South African Perspective

**Adedamola Owolade**[1]
AISA Young Graduate Scholar
Economist, Department of Economics
University of Pretoria
South Africa
E-mail: damolaowolade@gmail.com

**Sizwe Lindelo Snail**[2]
AISA Young Graduate Scholar
Attorney at Law at Couzyn Hertzog & Horak Inc.
Pretoria, South Africa
E-mail: Sizwes@couzyn.co.za

**ABSTRACT**

Sexual exploitation of children and adolescents in Africa and other countries has ceased to be a growing concern but has clearly become a visible reality. The internet has not only opened up new avenues for sexual predation but has also encouraged the organised and systematic sexual exploitation of vulnerable individuals in third world countries (UNICEF, 2008). Research has also illustrated that there is growing evidence of criminal activity related to the proliferation of imagery and other internet related exploitative practices (ibid). Other exploitative practices include the luring of children over the internet for sexual-orientated activities, child pornography and child sex tourism and prostitution which is particularly important in countries with a significant tourism sector relative to others. South Africa, Egypt and Tunisia are notable African countries with buoyant tourist influx (UNECA 2007).

It has also been argued that sexual exploitation contributes to missing children, sexual abuse and statutory rape cases. Mitchell and Wells (238-239:2007) looked at the possibility of mental health disorders which can be attributed to online sexual exploitation although causality was not established. The conclusion showed that victims of sexual victimization also showed signs of mental health issues. These include post-traumatic stress disorders, mood disorders, and substance disorder. The World of Works (2:2002) proposed that the problem of sexual exploitation could be rooted in more structural issues such as poverty, the breakdown of families, armed conflict, drugs and the increase in demand by drug abusers. This preceding views shows that sexual exploitation online could be and the effect of social problems.

The lack of and credibility of data limits an assessment of the true incidence of sexual exploitation through the internet. Some of the cited reasons include the willingness of the abused to report to the relevant authorities, if they exist in the first place. Even in the case were sexual exploitation is criminalised, the abused might not be informed or aware of where to make complaints. These reasons make it difficult to assess the extent of sexual exploitation, especially in emerging countries that aren't renowned for keeping statistics in general. Therefore, this presents challenges in conducting a study on online sexual exploitation. For this reason, the form of sexual exploitation this paper focuses on is that of child pornography given the harnessed international effort in combating this problem in recent times.

[1] B.Com -Hons-(UP) , M.COM (Candidate at UP)

[2] LLB (UP), LLM (Candidate at UNISA)

Countries have been forced to make legislative changes to their existing criminal law to incorporate and specifically deal with offence relating to child pornography. This paper seeks to investigate the key legal issues relating to child pornography with reference to the International Centre for Missing and Exploited Children's Report on Child Pornography (ICMTCRCP): Model Legislation & Global Review (2008) which offers a comprehensive collection on international legal instruments that address child pornography as well as Model Laws proposed for legal reform on child pornography. The paper will give South African legal perspectives on child pornography and compare them with the laws of African and a specific case study on Brazil

The aim of this research is to identify the incidence of online child pornography in South Africa. The extent of child pornography in South Africa will then be compared with countries with a similar income and social profile. The paper will also conduct a comparative legal survey on how lack of regulation and lack of law enforcement perpetuates the sustained occurrence of these immoral and illegal practices. The paper will also make conclusions and recommendations on international efforts by NGO's and multilateral agencies in regulating cyber-sex, combating and eradication of illegal online sexual practices

## INTRODUCTION

Online Sexual Exploitation (OSE) refers to any sexual related offence against anyone, especially children, directly or indirectly through internet technology (Butt, 2009). In order to contextualize the topic of online sexual exploitation (OSE), one needs to consider the internet's penetration and usage in South Africa compared to the rest of the world. It is conventional wisdom that the adoption of technology helps accelerate production and economic growth. It can also help improve on the sharing of culture and presenting a platform for a world without borders facilitating trade and knowledge transfer. However, there have been concerns of the negative[3] aspects of technology, especially the internet, in the world and Africa is very much implicated.

According to the End Child Prosecution, child pornography and the trafficking of children (ECPAT) and Interpol, the degree of OSE is extensive and is becoming a global problem. However, some quarters have raised concerns of freedom of expression and censorship with regard to proposed measures in curbing OSE (Sabrinho: 9, 2009). Given the many avenues in which people can publish personal information and interact with others on the internet, it would not be wayward to assume that regulation and control of access is not able to keep up with penetration rates and percentage increase in users globally. The next section looks at the some of the statistics regarding internet outreach in Africa compared to the rest of the world.

## BRIDGING THE DIGITAL DIVIDE

Table 1 shows the extent in which Africa is striving to bridge the digital divide. The percentage increase of internet usage in Africa is in excess of a thousand percent from 2000 to 2008 which is three times more than the rest of the world. This could be attributed to Africa catching up with the rest of the world given recent economic success stories and the buoyancy of the telecommunication sector. Table 2 shows that South Africa has about 10 percent access or penetration rate with a usage percentage growth of about 92 percent between 2000 and 2008. Morocco doubles the penetration rate in South African while Nigeria has about 7 percent access rate. However, both Morocco and Nigeria both have a usage growth rate in excess of 4000 percent each.

However, the African population accounts for about 15 percent of the world population. Internet usage in Africa is only 3.4percent of the world population. South Africa has 9percent of the African usage figures. Morocco and Nigeria combine to make up 30 percent of internet usage in Africa according to Table 2. The question is now the extent of OSE of children in South Africa. Five years preceding

[3] Internationally 27 750 child pornography websites were identified in 2005 according to HSRC 2005

2005, there were only 20 reported cases of persons possessing, distributing or manufacturing child abuse images which were investigated in South Africa according to HSRC 2007. Countries with high penetrations rates, like the US[4], have more records of OSE. This could prompt the idea that deeper outreach of the internet leads to higher incidence of OSE.

Table 1: Internet users in Africa and the World in 2008

| AFRICA REGION | **Population (2008 Est.)** | **Pop. % in World** | **Internet Users, Latest Data** | **Penetration (% Population)** | **Use Growth (2000-2008)** | **% Users in World** |
|---|---|---|---|---|---|---|
| Total for Africa | 975 330 899 | 14.50% | **54 171 500** | 5.60% | 1100.00% | 3.40% |
| Rest of World | 5 734 698 171 | 85.50% | **1542098608** | 26.60% | 332.60% | 96.60% |
| **WORLD TOTAL** | 6 710 029 070 | 100.00% | **1596270108** | 23.80% | 342.20% | 100.00% |

Source: www.internetworldstatsonline.com

Table 2: Internet users in South Africa and selected African countries 2008.

| Country | **Population (2008 Est.)** | **Internet Users Dec-00** | **Internet Users Latest Data** | **Penetration (% Population)** | **User Growth (2000-2008)** | **% Users in Africa** |
|---|---|---|---|---|---|---|
| Morocco | 34 343 219 | 100 000 | **6 600 000** | 19.20% | 6500.00% | 12.20% |
| Nigeria | 146 255 306 | 200 000 | **10 000 000** | 6.80% | 4900.00% | 18.50% |
| South Africa | 48 782 755 | 2 400 000 | **4 590 000** | 9.40% | 91.30% | 8.50% |
| Algeria | 33 769 669 | 50 000 | **3 500 000** | 10.40% | 6900% | 6.50% |
| Kenya | 37 953 838 | 200 000 | **3 000 000** | 7.90% | 1400.00% | 5.50% |

Source: www.internetworldstatsonline.com

## MEASURING ONLINE SEX OFFENCE AND THE DIFFICULTIES IN ATTAINING RELIABLE STATISTICS

After considering the level of usage of the internet in South Africa, one now needs to embark on the daunting task of accounting for the number of children who use the internet and have been exposed to inappropriate content and images. This is practically impossible but one can infer from existing or

[4] The biggest market for child pornography is the United States of America which it is estimated accounts for 85% of world sales according to HSRC2007.

secondary sources, as to level of internet usage by children. The usage of WAP (Web Access Point) enabled cellular phones also presents challenges since the avenues in which children can be online is no longer limited to the personal computer. Nevertheless, the Internet is being used for a diverse range of purposes including e-mail and chat; for homework tasks; to play games and listen to music; to get information about sports, entertainment and hobbies; to get health and medical information; and to shop according to Cocotti-Muller et al (136 :2006).Their study looked at the extent of exposure of children to inappropriate material and behaviour online and whether the use of blocking and filtering software reduces such exposure in Australia. Furthermore, the role that parental discussions about Internet safety might play in helping keep young people safe online is explored. Their results showed that males have more exposure and security measures such as filtering software had no effect on potential and actual exposure.

A survey was conducted by the Film and Publication Board (FPB) of South Africa in 2006. The aim of this survey, conducted among learners in the 13 to 17+ years age-group in randomly-selected schools in Cape Town, Durban and Johannesburg, was to provide an informed basis for the establishment and implementation of public policy initiatives and other measures not only to minimise children's exposure to such materials but also to empower them with the necessary skills to cope with any distress that they might suffer from involuntary exposure to disturbing, harmful and objectionable materials both online and offline. Some of the pertinent results of the survey showed that 64 percent have been exposed to pornographic images on the internet. Of those who have encountered pornography on the internet, 70 percent reported coming across such materials accidentally. More than half (60 percent) exchange addresses of pornographic websites with their friends. On mobile cellular phones: most children who participated in the survey (88 percent) have their own cellular phones. 81 percent reported knowledge of pornographic images on the phones of their friends and would, therefore, have seen such images. (FPB, 2006)

The HSRC shows the extent of manufacturing and distribution of child pornography in South Africa, the number of criminal cases in which child pornography played a role, and whether it is possible to establish profiles of perpetrators and children who are vulnerable to this form of exploitation. The research was conducted amongst children between the ages 10-12 years (Grade five to seven) and 13-15 years (Grade eight to nine) in Johannesburg, Durban and Cape Town. A total of 604 questionnaires and 37 in-depth interviews were completed.

The research study found that 22 percent of the children who participated in the study have been exposed to worrying content on the internet mostly of a sexual nature and nudity. 14 percent of chat room users in the age group have been exposed to distressing content in chat rooms and have had sexual advances made to them on line. 12 percent have been exposed to distressing content on cell phones mostly of a sexual nature. Seven percent have been exposed to distressing e-mail content which was mostly violent and sexual. The figures in the results of the FSB(2006) report suggests a higher frequency of OSE compared to the HSRC(2007).However, there could be other factors ,such as socio –demographic characteristics, which increases the risk of exposure to inappropriate content that could be dominant in the HSRC(2007) sample. These could include race, income group, education, and place of residence. Wolak et al (424, 2004) incorporated similar socio-demographic characteristics in their analysis in which the circumstances in which juveniles who were victims of OSE were assessed. Their results showed that higher income children, who lived with both parents in a suburbia environment, are at a higher risk.

## TYPES OF ONLINE SEXUAL EXPLOITATION (OSE) OF CHILDREN [5]

### Online enticement of children for sexual –orientated interaction

This occurs through the use of social network sites and chat-rooms where children are lured into sexual conduct which often results in physical contact between the offender and the victim. This involves the offender seeking the trust of the victim and then enticing the victim with gifts which eventually leads to the two meeting up in a physical world encounter. The pre- physical contact can also involve discussions of sexual nature and the sharing of pictures which might be sexual in nature. Finkelhor et al (114:2007) also explains OSE from this point of view but raises the argument of OSE, in this case, being tantamount to statutory rape.

### Child sex tourism and prostitution

The outreach of the internet with the low costs and ease of maintaining and updating a website has made created a platform to advertise and sell sex for hire services. Prostitution websites that offer sex services with contact information, and associated fees are appearing more frequent created by those promoting sex with minors and adults. Those in the tourism business, especially travel agents, have started specialising in sex tours which are advertised on the web. These kinds of services are particularly rife in countries where government enforcement against adult-child sexual encounters are negligent. These travel agents also provide access to brothels, sex clubs, and escort agencies in addition to their generic duties of airfare arrangements and accommodation services. Social network sites and chat rooms also provide patrons with experiences, exploits and cautionary advice to those wishing to travel abroad for the purpose of having sex with the under-aged.

The types of OSE preceding this paragraph involve physical contact between the offenders and the victims. Many countries, including South Africa, criminalise sexual activities between an adult and an under-aged person. This is mostly known has “statutory” rape. It is defeating for the purpose of this paper to learn that the recorded statistics in SA are not disaggregated to isolate the count of cases which were a result of OSE. This complicates the task of assessing the level of OSE in South Africa.

### Unwanted exposure of children to pornographic material and Child Porn.

It has become common for internet users to be exposed to pornography without searching for it. Children are not excluded from this group of users bombarded by pornographic material or “pop ups” advertising pornographic material. Children who run searches on their favourite pop stars can also be exposed to pornographic material involving look alikes of those they intended to look up. Misspelt URLs may also lead to websites which expose viewers to pornographic images.

Child pornography is any depiction of a child engaged in real or simulated explicit sexual activities. Technology such as computers and internet has simplified the creation, distribution and collection of child pornography. Collectors can also download child pornography from their homes with a sense of secrecy. Cell phones that are internet enabled have also contributed to the proliferation of child pornography. The content in these images varies from exposure of genitalia to graphic sexual abuse, such as penetration by objects, anal penetration, and bestiality. See figure 1 in Appendix A for further classification of OSE.

## PROFILE OF VICTIMS

According to the HSRC, it is difficult to establish a profile for children that are susceptible to OSE in South Africa. However, Finkelhor et al (118:2006) argued that girls are more vulnerable which is counter intuitive to the findings of Cocotti-Muller et al (2006). This is argued on the grounds that girls mature quicker than boys and tend to be sexually aroused or active before a boy of the same age. They

[5] O’leary, Robert., D’Ovidio, Robert. 2007. Online Sexual exploitation of children. The International Association of Computer Investigative Specialists. P.??

are also likely to get involved with older guys in order to explore their new found sexuality. The widespread stereotype and stigma that comes with being gay, encourages male homosexuals seeking solace on the internet. The internet also becomes a domain where they can meet partners and could potentially be exploited.

The world of works (2002) proposed that the problem of sexual exploitation could be rooted in more structural issues such as poverty, the breakdown of families, armed conflict, drugs and the increase in demand by drug abusers. This preceding views shows that sexual exploitation online could be and the effect of social problems. This proposed idea does not have any empirical backing which presents a gap for further research.

## INTERNATIONAL AND AFRICAN RESPONSE TO OSE OF CHILDREN

Child pornography is a multi-jurisdictional problem to which a global approach must be applied. Successfully combating child pornography and child exploitation on a global scale requires uniform legislation. (ICMTCRCP: 7:2008). The International Centre for Missing and Exploited Children's Report on Child Pornography (ICMTCRCP): Model Legislation & Global Review (2008) suggests that a comprehensive legislative strategy must be created to not only investigate but also prosecute offenders beyond the criminalisation of certain action by child-sex offender. The model legislation is broken down into 4 (four) parts namely: definitions, offences, mandatory reporting as well as sanctioning and sentencing. (ICMTCRCP: 1:2008). It is proposed that the definition of "child" be defines as anyone under the age of 18. This is due to the fact that although certain countries may regard consent to sexual acts at ages such as 14 and 16 years it is questionable whether their OSE would be condoned as they would in many instances not be major who may legally consent to OSE. (*Ibid*). It is also suggested that the meaning of "child pornography" include at a minimum, the visual representation or depiction of a child engaged in a (real or simulated) sexual display or act or performance.

The ICMTCRCP also states that mere ban on child labour incl. child pornography is not sufficient a country must specific offences in its penal code must be created and specific tough sanction (ICMTCRCP: 2:2008). It is also suggested by other commentators that simple possession, downloading or attempt to possess should also be criminally sactionable so as to deter the consumers of child pornography. (Vachs: 2006:1) as well as other incidence of sexual abuse in the online world. Other suggestions are also penalising those who make child pornography available as well as parents who allow their children to be victims of OSE but also those who commit grooming offences such as "online enticement" or "normalizing" the child to child pornography. (ICMTCRCP: 3:2008).

The report also advises that states should try and enact mandatory reporting procedures of OSE of children of 3(three) classes of individuals or organisations that must be required to report suspected OSE and in particular OSE of children. These are namely: people who in their professional capacity come into contact with children, people or organisation that may not specifically be in contact with children but have been exposed to child pornography in course of their duties and lastly ISP, banks and credit card companies. The report also seeks ways to deal with child offender of child pornography and also to deal with incidence of repeat offenders. (ICMTCRCP: 4-5:2008).

There are three main international legal instruments that address child pornography: the Optional Protocol to the (U.N.) Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography; the Council of Europe Convention on Cyber crime; and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

While the Convention on the Rights of the Child (CRC) aims to ensure a broad range of human rights for children – including civil, cultural, economic, political, and social rights– there are Articles within the CRC and an Optional Protocol to the CRC that address child sexual exploitation. (ICMTCRCP: 7:2008).Article 34 of the CRC clearly states that:

> "States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent…[t]he exploitative use of
> children in pornographic performances and materials."

The CRC Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (Optional Protocol) entered into force on 18 January 2002. This piece of international law is more specific to child pornography. Article 2(c) defines "child pornography" as "any representation, by whatever means, of a children engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes." Article 3(1) requires State parties to criminalize child pornography, whether committed domestically or transnationally, on an individual or organized basis. Article 3(1) (c) requires State Parties to criminalize simple possession regardless of the intent. (ICMTCRCP: 7-8:2008).

In the European Union Cyber crime law is primarily based on the Council of Europe's Convention on Cyber crime (CCC) (November 2001). South Africa has signed but did not ratify the Convention. Under the convention, member states are obliged to: criminalise various illegal computer activity and most importantly for the purposes of this discussion the prohibition and prosecution of offenders of online child pornography related offences such as possession, distribution, procuring and or the producing of child pornography. (See Article 9 of the CCC relating to offences related to child pornography)[6]. For the purpose of Article 9(2) the term "minor" shall include all persons less than 18 years of age. States may, however, require a lower age-limit, which shall be not less than 16 years.

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse (Child Protection Convention) is the most recent international legal instrument aimed at combating OSE of children. The Child Protection Convention focuses on ensuring the best interests of children through prevention of abuse and exploitation, protection and assistance for victims, punishment of perpetrators, and promotion of national and international law enforcement cooperation. (ICMTCRCP: 9:2008).

From an African perspective Olowu suggests that an integrative pan-African approach concerning cyber-criminality may be the only viable way to effectively combat the phenomenon. To this end, the African Union (AU), through its numerous technical agencies and commissions could assume responsibility for designing the framework for a continent-wide legal approach, after all, responding to this continent-wide challenge, even though not specifically mentioned in its founding instrument can be read into it. (Olowu: 2009:9) He goes on to state that the Constitutive Act of the AU, 2001, clearly

[6] 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;
b offering or making available child pornography through a computer system;
c distributing or transmitting child pornography through a computer system;
d procuring child pornography through a computer system for oneself or for another person;
e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;
b a person appearing to be a minor engaged in sexually explicit conduct;
c realistic images representing a minor engaged in sexually explicit conduct.

outlines the objectives of the AU which inter alia relate to legal policy formulation as a whole and may be read into as applying to the combating and enforcement of child OSE. (Ibid). The Objectives of the AU are to:

(a) achieve greater unity and solidarity between the African countries and the peoples of Africa;

(b) defend the sovereignty, territorial integrity, and independence of its Member States;

(c) accelerate the political and socio-economic integration of the continent;

(d) promote and defend African common positions on issues of interest to the continent and its peoples;

(e) encourage international cooperation, taking due account of the Charter of the United Nations and the Universal Declaration of Human Rights;

(f) promote peace, security, and stability on the continent;

(g) promote democratic principles and institutions, popular participation and good governance;

(h) promote and protect human and peoples' rights in accordance with the African Charter on Human and Peoples' Rights and other relevant human rights instruments;

(i) establish the necessary conditions which enable the continent to play its rightful role in the global economy and in international negotiations;

Olowu concludes that by applying the basic rules of statutory interpretation, it is safe to posit that a valid platform exists in the AU's Constitutive Act to mandate its structures to engage in formulating a comprehensive initiative against cyber-crimes in Africa. (Ibid at 10)

## SOUTH AFRICAN LAWS THAT PROHIBIT OSE

After many years of legal uncertainty Parliament enacted the Electronic Communications and Transactions Act [7] (ECT) which comprehensively deals with Cyber crimes in Chapter XIII and has now created legal certainty as to what may and not constitute Cyber crime. Unfortunately no express cyber pornographic crime is stipulated in the ECT. One must however, note s3 of the ECT (its interpretation clause) which does not exclude any statutory or common law from being applied to, recognizing or accommodating electronic transactions – in other words the common law or other statues in place wherever applicable is still in force and binding which has the result that wherever the ECT has not made specific provisions for criminal sanction such law will be applicable. (6:2009: Snail)

Specific reference should also be made to the common law saving provision in Section 91 which confirms that the common law still prevails were no specific provision has been made for a crime in the ECT. This is important when dealing prosecutions of child pornography crimes as there is no express provision against child cyber pornography in the ECT. It is submitted that prior to the enactment of the ECT, that the common law and statue at that time could be extended as widely as possible as to cater for the arrest and successful prosecution of online child porn offenders. One can easily apply the common law crime of indecency to the creation of online child pornography or unlawful dissemination of child porn.

Possession and distribution of child pornography can also be prosecuted in terms of the Films and Publication Act [8] which provided in its definition of publication that a publication is:

[7] 25 of 2002

[8] Act 65 of 1996

> "(i) any message or communication, including visual presentation, placed on any distributed network including, but not confined to, to the internet.

The application of the previously codified and common law crimes was sometimes regarded as an academic expedition and caused great uncertainty as courts and prosecutors were not keen to do adventurous prosecutions. Gordon states that in 1998 the then Eastern Cape Attorney General was loath to prosecute a man who had placed child pornography on his website as the said act was not in force. This caused a general outcry in the community and the legislature was forced to brig the said act into force in order to fill in the *lacunae* that was existing in the law. (Gordon: 2000:439)

In terms of section 27 (1) and section 28 of the said legislation if:

> "anyone creates, produces, imports or is in possession of a publication or film which contains scenes of child pornography, he shall be guilty of an offence."

Section 27 (1) and Section 28 refer to child pornography publication and child pornography in films respectively. Gordon also notes that the act may also extend to "pseudo-pornography" as found in animated pornography. (Gordon: 2000: 440) Section 25 and section 26 respectively also prohibit the decimation of child pornography in films or publications.

One interesting provision of the ECT which is not contained in the chapter dealing with Cyber crimes is the take-down procedure of websites that may contain unlawful activity which is currently being administered by ISPA (Internet Service Providers Association available online at http://www.ispa.org.za). In terms of Section 75 (1) (c) of the ECT an ISP would not be liable in law to any 3rd party for the contents of its client's website if it has complied with a take down notice as stipulated by section 77 (a) – (h) which sets out a procedure and grounds[9] why a website should not continue being made available ban ISP (Internet Service Provider).

It appears that save for the take down procedure, as stipulated in section 77 above has only introduced one real new legal in the ECT to tool to curb online child pornography related offences and that South African statute and common law relating to criminal law can and must be widely applied to online child pornography offences. With the above having been said the ECT does give us an idea as to how

[9] Take-down notification in terms of 77 of the ECT:

(1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated include-

(a) the full names and address of the complainant;

(b) the written or electronic signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of

(e) the remedial action required to be taken by the service provider in respect of telephonic and electronic contact details, if any, of the complainant;

(8) a statement that the complainant is acting in good faith;

(h) a statement by the complain that the information in the take-down unlawful activity; the complaint notification is to his or her knowledge true and correct; and

(2) 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 notification.

(3) A service provider is not liable for wrongful take down once a notification has been received

a Court may found jurisdiction for it to hear a child pornography offence in Section 90 of the ECT. Sec 90 of the Act gives South African courts the jurisdiction to try offences arising from actions where an offence is committed in the republic, any act in preparation for the offence takes place in the republic, any part of the offence is committed in the republic, the result of the offence has effects in the republic, the offence is committed in the republic, by a person carrying on business in the Republic or when the offence is committed on board any ship or craft registered in republic.

On the other hand the South African Common law can also be applied with regard to the common law and now also statutory defined definition of rape and or other indecent a sexual act with children under age of 18 years. A refreshing thought is that according to the International Centre for Missing and Exploited Children's Report on Child Pornography (2008:28) it is notable that South Africa is one of the 29 (twenty-nine) countries in the world that has legislation sufficient to combat child pornography offences in terms of the 5 (five) core legal provisions that a country must comply with as discussed in the section dealing with international responses to OSE in this paper.

**BRAZILIAN RESPONSE TO OSE IN PARTICULAR CHILD PORN**

In 2003 according to ratings disclosed by Ibope / NetRatings about Brazil it stated that "the young Brazilian Internet user is the second largest user of the web around the world" and that children of six to eleven years on average 4 hours and 51 minutes using internet. Probably, with the explosion of the Internet in Brazil, with more than 40 million users currently, the numbers have since changed exponentially. (Sobrinho: 2009:4) Sobrinho shows in his case study of Brazil cases that sexual exploitation involving children, through dissemination of photos, videos, texts, images and pictures of pornographic content on sites such as Orkut (Google's), MySpace and Facebook, with emphasis on the first in countries like Brazil is a rife practice and that law enforcement has to step in to protect victims.. (Sobrinho: 2009:8)

In Brazil, the legal definition for child pornography was adopted in 2004 under Article 2 (c) of the Optional Protocol to the Convention on the Rights of the Child on the sell of children, child prostitution and child pornography, adopted in New York on May 25, 2000. This Protocol as previously discussed defines child pornography as:

> "any representation, by whatever means, of a child engaged in explicit sexual activity, real or simulated, or any representation of the sexual organs of a child for primarily sexual purposes",

Sobrinho argues that this definition can be applied to unlawful conduct on the Internet relati8ng to OSE of children. Sexual exploitation on the Internet in Brazil often involves young children up to 12 years and adolescents aged up to 18. The advent of the Internet did not reduce the problems that occurred in the real world, unlike, added all aspects to issues of sexual exploitation involving much larger proportions. For example, photos or a video of a sex scene involving children or adolescents which were previously restricted to one city are now made available on a global network accessible to an incalculable number of people. (Sobrinho: 2009:9)

There are no official records on the number of complaints involving child pornography on the Internet. In March 2008, a Non Governmental Organization - NGO, called SaferNet, which collects reports of child pornography on the Internet in Brazil, reported that "around 90% of complaints of child abuse registered in Brazil last year [1997] had relationship with the content of Orkut [...] ". Another shocking report indicated that "in total, the SaferNet received 267,470 complaints about child pornography in 2007, a high of about 120% over the previous year [1996]" which indicates the willingness of users to denounce abuses committed, mainly on the site of relationship. (Sobrinho: 2009:10)

The repercussions of online OSE were clearly illustrated with the cases of online child pornography on Orkut in Brazil which got to unimaginable proportions. The Senate of the Republic started a Parliamentary Commission of Inquiry in March 2008 to investigate the cases of paedophilia and child

pornography on the Internet. Sobrinho points out that most complaints in (almost all complaints) were against Orkut. The Commission of the Senate approved the breach of confidentiality of Orkut albums with pornographic content and they restricted access to these sites to other users. (Ibid)

The company Google that maintains a subsidiary in Brazil initially resisted to provide confidential information contained in 3,261 Orkut albums that contained content and images of child pornography. However when the Parliamentary Commission of Inquiry, which has judicial powers, stepped into the legal fiasco Google decided to collaborate. In r previous attempts Prosecutors of the Republic of Brazil were denied access to content on the album, under the argument that because of Google is a U.S. company, with the database in the United States of America, would be subject to the jurisdiction of U.S. laws, which ensure the freedom of expression and not to Brazilian law. (Sobrinho: 2009:10-11). More than 500 of the users on Orkut were detected as scenes of paedophilia related cyber crime. In November 2008, the President of the Brazil signed the new national law with stronger punishments for child pornography or other wise known as OSE. (Ibid)

## CONCLUSION AND RECOMMENDATION

The Internet industry does not like to admit how much it is being supported by the sex industry, but a few indicators are revealing. The sex industry is among the top five groups buying state-of the- art computer equipment. Sex industry businesses were the first to buy and use expensive T3 phone lines that transmit compressed, high-resolution images. One of the largest Internet companies in the world, Digex, whose largest customer is Microsoft Corporation, has a sex industry site as its second largest customer (Hughes:36: 2000). This particular point shows that the one might not be too off the mark to assume that high internet penetration rates, or larger internet markets, tend to have higher incidence of OSE. Given the low internet penetration in SA, how much of a problem is OSE? It has already been show that this problem cannot be quantified. However, as internet usage increases, the possibility of an increase in OSE incidence is eminent and public policy should be geared towards the protection of the vulnerable.

It is clear that international co-operation is absolutely imperative in order to combat and enforce laws against OSE, in particular OSE of children. International organisations SPLEKNO OKO, The International Centre for Missing and Exploited Children's, the UN and the European Council have gone a long way to try and achieve global uniformity with regards to enforcement and penalties for cyber crimes related to OSE. The case study of Brazil clearly shows how lack of regulation and co-operation may result in the commission of a plethora of OSE related sexual offences. This paper clearly show how national legislative measures such as those in South Africa and recently Brazil, together with international co-operation are the first right step into reducing and eradicating this modern scourge on our society. It is still unclear what African solution is being drafted to deal with OSE on a continent level but clearly the AU constitutive Act places a duty on member states to act on OSE as it is increasingly becoming a problem.

## REFERENCES

**Articles:**

Cocotti-Muller, Dayana., Elias ,Kristy. A., Fleming ,Michele J., Greentree ,Shane., Morrison, Sarah.(2006)."Safety in Cyberspace: Adolescents' Safety and Exposure Online". *Youth Society* 2006; 38; 135

Finkehol,David., Mitchell, Kimberly., Wolak ,Janis. J.D. 2004."Internet-initiated Sex Crimes against Minors:Implications for Prevention Based on Findings from a National Study". Journal of adolescent Health. Vol, 35.

Gordon, Barrie (2000) "Internet Criminal Law" in *Buys R, Cyberlaw @ SA: The law of the Internet in South Africa*, at p.440.

Hughes,D.M 2000. "Partners in Global Sexual Exploitation". *IEEE Technology and Society Magazine*. Spring issue 2000

Krone, Tony. (2004). "A typology of online child pornography offending".in *Australian institute of Criminology*. No. 279,

Mitchell,K.J., Wells, M. 2007. "Youth Sexual Exploitation on the internet: DSM-IV Diagnoses and Gender Differences in Co-ocurring Mental Health Issues".Child and Adolescent Social Work Journal, Vol.24,No.3

O'leary, Robert., D'Ovidio, Robert. (2007) "Online Sexual exploitation of children". in *The International Association of Computer Investigative Specialists*..

Olowu, Dejo (2009) "Cyber-Crime and the boundaries of domestic legal responses: Case for an exclusionary framework for Africa" in *Journal of Information, Law & Technology*, 2009(1)

Snail, Sizwe (2008) "Cyber crime in the context of the Electronic Communications Transactions Act, in *Juta Buiness Law* 16(2), p.65.

Snail, Sizwe (2009) "Cyber Crime in South Africa-Hacking cracking and other unlawful online activities" in *Journal of Information, Law & Technology,* 2009(1)

Wolak, Jamie., Finkelhor, David.,Mitchell, Kimberly., Ybarra, Michele.(2008). "Online "Predators" and their victims: Myths, Realities, and Implications for Prevention and Treatment" in *American Psychologist,* February-March 2008

**Books , Reports & Policy Documents :**

Buys R, Cyberlaw @ SA: The law of the Internet in South Africa, 2000

Basson, Antoinette. Chetty, Iyavar (2006) Report on internet usage and the exposure of pornography to learners in South African Schools. Film And Publication Board,

Butt, David.(2009) Investigating internet child exploitation poses complex challenges. Kid Internet Safety Alliance,

Dawes ,Andrew., Govender, Advaita.(2007) .The Use of children in pornography in South Africa. HSRC Report

Economic Report on Africa 2007. United Nations Economic Commission for Africa. UN

International Centre for Missing and Exploited Children's Report on Child Pornography: (2008) Model Legislation & Global Review

Van der Merwe et al. (2008) Information and Communication Technology Law,

World of Works. (2002) Sexual Exploitation of children. No. 42, March 2002. *ILO*

**Conference Papers:**

Fourth Annual Meeting of the Asia-Pacific Forum: Child Pornography and the internet. Summary of conference proceedings

Sabrinho, Arnaldo (2009) The cases of the Cyber child pornography in Brazil : International legal issues of jurisdiction and privacy . Paper presented at ISSCIM 2009, 1st Conference on Cyber crimes and International Co-operation, Jessoa Pessoa, Brazil. 21st May 2009.

UNICEF working papers and conference contributions to the World Congress against the Sexual exploitation of children (I-III)

**Legislation:**

Constitutive Act of the AU, 2001

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual

Abuse Lanzarote, 25.X.2007, accessed at http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

Electronic Communications and Transactions Act, Act 25 of 2002

EU Convention on Cyber Crime, 2001 (ETS 185)

Films and Publication Act, Act 65 of 1996

Optional Protocol to the (U.N.) Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography G.A. Res. 54/263, Annex II, U.N. Doc. A/54/49,

**Online:**

Vachss, Andrew (2009) Let's Fight This Terrible Crime against Our Children (accessed on the 9th June 2009 at http://www.parade.com/articles/editions/2006/edition_02-19-2006/Andrew_Vachss )

.

## APPENDIX A

**Figure 1: Typology of online child pornography**

| Type of involvement | Features | Level of networking by offender | Security | Nature of abuse |
|---|---|---|---|---|
| Browser | Response to spam, accidental hit on suspect site—material knowingly saved | Nil | Nil | Indirect |
| Private fantasy | Conscious creation of online text or digital images for private use | Nil | Nil | Indirect |
| Trawler | Actively seeking child pornography using openly available browsers | Low | Nil | Indirect |
| Non-secure collector | Actively seeking material often through peer-to-peer networks | High | Nil | Indirect |
| Secure collector | Actively seeking material but only through secure networks. Collector syndrome and exchange as an entry barrier | High | Secure | Indirect |
| Groomer | Cultivating an online relationship with one or more children. The offender may or may not seek material in any of the above ways. Pornography may be used to facilitate abuse | Varies—online contact with individual children | Security depends on child | Direct |
| Physical abuser | Abusing a child who may have been introduced to the offender online. The offender may or may not seek material in any of the above ways. Pornography may be used to facilitate abuse | Varies—physical contact with individual children | Security depends on child | Direct |
| Producer | Records own abuse or that of others (or induces children to submit images of themselves) | Varies—may depend on whether becomes a distributor | Security depends on child | Direct |
| Distributor | May distribute at any one of the above levels | Varies | Tends to be secure | Indirect |

Source: Australian institute of Criminology

# Is there a White-Hat Exception to the Computer Fraud and Abuse Act?

**Milton H. Luoma, Jr.**
Assistant Professor
Metropolitan State University
St. Paul, Minnesota

**Vicki M. Luoma**
Associate Professor
Minnesota State University
Mankato, Minnesota

**ABSTRACT**

Three MIT students were planning to present details on how to "get free rides for life" on the Massachusetts Bay Transit Authority (MBTA) transit system at a conference. When a vendor attending the conference notified the MBTA of the pending presentation, the MBTA sued the students and MIT alleging a violation of the Computer Fraud and Abuse Act. The defendants claimed that they were providing a service to the MBTA and the public as white-hat hackers by exposing system vulnerabilities. While the case was ultimately settled out of court short of trial, important legal issues were raised that will likely arise again in the future under similar circumstances. The primary legal issues include whether the acts complained of were a violation of the Computer Fraud and Abuse Act. Further, was a prior restraint of publication of the security vulnerability an appropriate action to be considered by the court? This paper addresses these issues and concludes that the actions of the students were indeed a violation of the Computer Fraud and Abuse Act, and further, a prior restraint of the publication of such security vulnerabilities would be appropriate.

## INTRODUCTION

The more computer forensic skills a person develops the more the issue of ethics must be addressed. It is no longer what skills a person has but how those skills should be used. Almost from the beginning there is a debate on whether there can be a white hat exception to hacking and whether a black hat hacker can be redeemed as a computer security consultant. Can there be a distinction ranging from White to Gray to Black hat hacking, or is all hacking wrong? If there is a distinction between types of hackers are there any guidelines as to how the make that assessment? Should the determinative factor be the motive behind the hacking incident, or whether the hacker gains financially from the hacking, or is it how much it cost the victim? White hat hackers claim that they only break into companies' systems merely to alert them to security breaches. If that is the case, should the company have prior notice of the attempt? In the past, hackers of all colored hats have been hired away as security experts. "Thomas Patterson, the former regional partner for Deloitte & Touche Security Services Group, likened the practice of hiring ex-hackers to placing a fox in a henhouse." (Germain, 2004). James Harrison, co-founder of Invisus an Internet security firm said he does not see much difference between the white hats or the black hats; they are all breaking the law. (Germain, 2004).

The debate on whether there is actually a distinction between white hat hackers and black hat hackers has been titled cyber conflict by Gadi Evron, the well-known botnet hunter who works for Beyond Security. (Messmer, 2007) In the United States and in most countries hacking is a felony-level crime. It is legal only when done by request or prior knowledge and consent of the organization being hacked. (Wilbanks, 2008).

In a study conducted by Young, Zhang, & Prybutok, at the DefCon conference in Las Vegas they found "that hackers justify their behavior, perceive a low level of social sanction, a high level of severity punishment from the court but a low likelihood of getting caught and receiving the punishment. Hackers also perceive a relatively high utility value resulting from engaging in illegal hacking activities." (Young, 2007)

Universities teaching such courses normally have an ethical guide for students when confronted with the white hat versus black hat debate. At Massachusetts Institute of Technology there is a course taught by Ronald Rivest entitled "Network and computer Security. " The course consists of approximately five problems and a final project that are completed in teams. (Rivest, 2009).

The syllabus for the 2009 Section 12 version of the course contains the following provision:

> This is a course on Network and Computer Security. Although the course is primarily concerned with techniques that are designed to increase the security of networks and computer systems, a proper understanding of those systems requires that you be versed in their vulnerabilities and failings as well. Nevertheless, unless you have explicit written authorization from the owner and operators of a computer network or system, you should never attempt to penetrate that system or adversely affect that system's operation. Such actions are a violation of MIT policy and, in some cases, violations of State and Federal law. Likewise, you should refrain from writing computer viruses, worms, self-reproducing code, or other kinds of potentially damaging software for this course unless you have explicit, written approval for the specific type of software that you wish to create. These kinds of programs are notoriously difficult to control and their release (intentional or otherwise) can result in substantial civil and criminal penalties. We strongly recommend that you consult the Athena Rules of Use at http://web.mit.edu/olh/Rules/,and Section 13.2 of the MIT Policies and Procedures \Policy on the Use of Information Technology" at http://web.mit.edu/policies/13.2.html.
>
> Finally, we recommend that you read and review the ACM Code of Ethics and Professional Conduct which can be found online at http://www.acm.org/constitution/code.html. (Or Google for "acm ethics".) We expect all students in this class to follow the guidelines presented in this document, and in the documents just cited. If you are in doubt about the legality or ethics of any activity related to this course, please consult the staff before undertaking any such activity.

Such a guideline to students is not only pertinent but necessary when teaching students about computer and network security. Students must know what is acceptable.

**FREE SUBWAY RIDES FOR LIFE**

On July 30, 2008 a vendor called the Massachusetts Bay Transportation Authority (MBTA) to alert them to an advertising promising "Fee Subway Rides for Life" on the MBTA. The MBTA found internet advertising for an upcoming presentation at DEFCON 16 conference which read:

> Want free subway rides for life? In this talk we go over weakness in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magastripe card we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. WE will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote to perform these attacks. (Docket No. 20, Ex 6)

DEFCON is the largest hacker conference with attendance of approximately 7,000 people. DEFCON stated purpose is to give hackers an opportunity to learn and to explore. The conference warns participants not to do anything illegal because the conference usually as many under cover law enforcement individuals. (Defcon Communications Inc, 2009)

The conference slides are available online for anyone who chooses to download them. Jeff Moss, now known as Dark Tangent founded the DEFCON conference and Black Hat. He has recently been named to the Homeland Security Advisory Council. (Zetter, 2008) Jeff Moss was a high school hacker, specifically a phone phreaker, who hacked into the telephone system to make free telephone calls. Moss defends DEFCON as opportunity for mentoring young hackers to be more ethical. (Zetter, 2008) Moss reports that most of his former hacker friends are now heads of security firms and these older hackers can provide valuable role modeling for younger hackers. (Zetter, 2008)

Jeff Moss stated that the hacking problem will never get better because there "are more people coming out of college who know how to program – but not securely – than there are people who know how to find the problem and fix them." (Zetter, 2008).

In this same interview Moss is asked specifically:

> "Some hackers claim they're benefiting security by hacking into systems and exposing vulnerabilities. Do you agree? **Moss:** I don't think that's valid. If you want to learn how to break into systems, you and your friends have enough computers that... you can build a network and break into it all day long without affecting anybody. You can simulate it." (Zetter, 2008)

Yet the very reason the MIT presentation was accepted for presentation is because the presentation promised to provide a detailed instructions with codes.

Reviewing this internet site was the first notice the MBTA had that their system had been hacked. The MBTA discovered this presentation was being made by three MIT students at the DEFCON conference. Further research discovered that there was also a promise that the presenters would present several attack methods that would completely break the Charlie Card." (Docket 20, 7)

The MBTA's automated fare collection system (AFC System) relied on CharlieCard Passes and Charlie Ticket passes for payment to the MBTA. The AFC system has installed a Fare Media System which was supposed to security features which would prevent unauthorized personnel from manipulating the system. The Fare Media system cost over $180 million to install.

**THEY GOT AN A!**

The students were enrolled in the Network and Computer security class mentioned above at MIT and it was taught by the renowned Professor Ronald Rivest. Rivest was one of three creators of the modern RSA public key encryption. As part of this class, Zach Anderson, RJ Ryan and Alessandro Chiesa were in a team and for their final project on the security vulnerabilities in the AFC's Fare Media System. As a result of their studies they prepared a paper and received an A in the class.

In the 2009 syllabus it requires students to obtain approval of their topic before conducting research. It also cautioned the students that they may not breach anyone security without permission of the company. (Rivest, 2009). It is unknown if the 2008 syllabus contained the same safeguards and approval but certainly by 2009 it did.

On May 14, 2008, Zach Anderson made a formal submission seeking selection of their research to be presented at the 2008 DEFCON Conference. (Third Mahony Decl.,1, at MBTA1-2). The DEFCON Conference is the oldest and largest hacker convention in the World. The students' submission was entitled "The Anatomy of a Subway Hack: Breaking Crypto RFIDs and Magstripes of Ticketing Systems." The submission also promised to release a new tool and to provide at least two demonstrations and five separate releases of software code.

Like all DEFCON applicants, presenters must sign a contract with DEFCON that grants all attendees of the conference the unlimited right to use the materials presented for all purposes. (MBTA)

In addition the MIT students had to grant DEFCON the right and permission to "duplicate, record and redistribution this presentation including but not limited to the conference proceedings, conference CD, video audio , hand outs to the conference attendees for educational, on-line and all other

purposes."(MBTA 4-5)

Once the MIT students were selected as conference speakers they made their slides available for download from the web and freely downloadable to anyone. Then in effort to advertise their presentation at DEFCON 16 the MIT students started advertising on the web by claiming they could provide the ability for "Free Subway Rides for Life."

The conference was not a requirement of the class and the student had failed to notify the MBTA that had hacked into their system, that they were going to do a presentation or provide information concerning protecting the system.

**SYSTEM IN CHAOS**

The MBTA immediately notified the MIT students that they would like to meet with them. The first contact between the students did not occur until July 31 and a meeting was not scheduled until August 4. At this meeting coordinated by their professor, the students denied ever hacking into MBTA system. The MIT students also assured MBTA and law enforcement that they would withhold key elements that would allow others to exploit the MBTA system. The MIT students also agreed to provide the law enforcement with a paper explaining vulnerabilities in the MBTA system. The students did not tell the law enforcement that they had already sent the documents to the conference nearly a month before this meeting with the MBTA. The students did promise to participate in a conference call on August 7. Despite the promise, the MIT students did not send the materials or participate in the conference call. After being contacted, the students then agreed to provide the information the next day. Then the students called and said on the advice of counsel they refuse to provide the information.

**THE TEMPORARY RESTRAINING ORDER**

The MBTA brought a motion for a temporary restraining order and recovery under the Computer Fraud and Abuse Act. Normally temporary restraining order is sought ex parte. Ex parte is without telling the adverse party that you are seeking to restrain them. A party can not receive a restraining order without an underlying lawsuit. (Rule 65) In this case MBTA was suing the students and university under the Computer Fraud and Abuse Act for misuse of a computer. Before the court enters a temporary restraining order the court must consider four factors: The plaintiff must establish that have a substantial chance of success on the merits of the case, they must show that they will suffer irreparable injury unless the injunction issues, the threatened injury outweighs any injury the relief would cause to defendant and the injunction is not adverse to the public interest. (Valley Cmty Pres. Comm'n Minetta, 373 F.3rd 1078, 1083 (10th Cir 2004)

In this case a restraining order was entered on August 9, 2008 and was set to expire on August 19, 2008 the date the MBTA had a motion for a permanent injunction. A permanent injunction is also in Rule 65. (Federal Rules of Civil Procedure, 2007) Unlike a temporary restraining order, preliminary injunction requires notice to the other party. To obtain a permanent injunction preventing the MIT students from publishing or speaking about their hacking project MTBA must show first that there is a probability of success on the merits and a possibility of irreparable injury in the injunction does not enter (Chalk v United States, 1988).

The restraining order prevented the students from presenting at the DEFON conference. At the injunction hearing the MBTA attorneys argued that it would take approximately five months to correct the problem discovered by the students. Further, if the hackers' information were made public the MBTA could face millions in losses. The student countered by arguing their hacking project actually contributing to the public welfare by exposing critical vulnerabilities in the transit system.

**THE COST**

The Boston MBTA received a grant to upgrade their subway system and they installed the automated fare system cost system, called the Charlie system. The new system had two payment methods, the

CharlieTicket and the CharlieCard. The CharlieTicket is a paper-based pass with a magnetic strip. The user brings the Ticket's magstrip into contact with a reader in the fare gate by swiping the Ticket past the designated reading head. The user can add or store value on the ticket for future use. CharlieCard pass is a plastic card that includes an integrated circuit with computer chip information. The card can store value on it. This system also allows the user to manage their account online. Eighty-eight percent of the riders use the plastic pass. These cards provide $475,000 per weekday in revenue. The average weekday ridership for the entire system is approximately 1.4 million passenger trips

The plaintiff sought relief under CFAA, 18 U.S.C. 1030, Conversion, Trespass to Chattels but this paper is on the Computer Fraud and Abuse Act.

## COMPUTER FRAUD AND ABUSE ACT

In response to the increase in computer crimes congress passed the Computer Fraud and Abuse Act (CFFA). (Computer Fraud and Abuse Act , 1986, amended 1986,1994,1996, 2001) The was act was first passed in 1984 and amended several times including 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. The Identity Theft Enforcement and Restitution Act Section (b) includes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to do so. The original purpose was to protect computers from the growing number of Hackers emerging in 1980's. The many changes in the law include computer activities that range from knowingly accessing a computer without authorization or exceeding authorized access to the transmission of a harmful component of a program, information, code, or command. " (Computer Fraud and Abuse Act, 1984, amended 1994)

Originally the act only covered Government computers but was amended numerous times until eventually covered all computers that could be involved in interstate commerce. In 1996 section G was added to the act that included a civil section to the act. It reads:

> g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware. (Computer Fraud and Abuse Act, 1984, amended 1994)

The computer fraud and abuse act also covers a person who knowingly causes the transmission of a program, information code or command to a computer or computer system. Thus, the issue becomes whether the Charlie Card standing alone constitute a computer within the meaning of Computer Fraud and Abuse Act.

## LEGAL HISTORY

Since the first civil case found a civil abuse of the Computer Fraud and Abuse Act, in the Shugart Case, the courts have found more abuses of the Computer Fraud and Abuse Act. (Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 2000). Recent cases have involved whether just accessing a computer site against the user instructions is enough to be a violation of the CFAA.

In a 2008 case Facebook, Inc sued StudiVZ, a German version of Facebook. In this case, Facebook claimed that StudiVZ violated their computer user policy which read: "You understand that the Web

site is available for your personal, non-commercial use only. " (Facebook, Inc. v Studviz, Ltd et , 2008) The creators not only admitted signing on as a guest and agreeing to the terms but also that they copied the Facebook site except for the background color. This case has not been resulted. In another case alleging violation of the computer fraud and abuse act, Financial Times Limited sued the Blackstone group because a senior official made a single subscription to the Financial Times available online to thousands of its employees in violation of its subscription agreement. The Financial Times operates a network of computers which it grants limited authorization by use of cookies and user credentials. Further with an individual subscription Financial Times only grants one person to access Financial Times. Financial Times alleges that employees at Financial Times intentionally assessed Financial Times computers without authorization. (Financial Times Limited v The Blackstone Group, L.P. and John Does 1-100, 2009). Although neither of this cases have had a final resolution it shows the trend towards arguing improper assess has been alleged to violate the Computer Fraud and Abuse act.

In another case Craiglist sued George Berz, d/b/a as adbomber, for using the Craiglist site either without authorization or accessing the computer in excess of his authorization. In this case Berz created a program that allowed users to repetitiously post duplicate ads in multiple categories and in multiple geographic areas which circumvented craiglist security measures. (craiglist,Inc.v Bertz, 2008). In a Ticketmaster case, Ticketmaster claimed that the defendant RMG Technologies developed and marketed automated devices that circumvented Plaintiff's access control allowing thousands of automated requests and preventing the intended customers from accessing the website and allowing the defendant's clients to purchase large quantities of tickets in violation of Ticketmaster's policies. (Ticketmaster LLC v RMG Technologies Inc et al, 2007) In all of these cases the Plaintiff's alleged over $5,000 dollar loss. In the Ticketmaster case, Ticketmaster won against RMG but not under the Computer Fraud and Abuse Act since they could not prove the $5,000.00 loss. In another case, Harold C. "Hal" Turner sued 4Chan.org and others for posting unauthorized copies of his radio program and attacked Hal's servers making it unavailable and placed orders for goods, services and merchandise in Hal Turners name. Hal alleged the computer was protected because the computer was used in interstate commerce. Turner also claimed that its computer was flooded with over 100 times the normal inbound data which it had to pay for. As a result of these attacks the Plaintiff had to shut off his web site. The message received was "We will not stop until you shut down your web site and your radio show." In another case MySpace sued Optinrealbig and Scott Richter for sending millions of spam bulletins through network by misappropriating login names and passwords from MySpace users. (MySpace Inc v Optinrealbig.com LLC et al, 2007) An Arbitrator awarded plaintiff's $6.08 million dollars including $4.8 million in compensatory damages.

In Sam's Wines & Liquors, Inc v Hartig, Sam's Wines alleged that Hartwig accessed their computer and obtained customers lists and email them soliciting. The court found that Hartig did access a protected computer without authorization and that Sam's did have a "loss" under the CFAA. However the court found that Sam's Wine was unable to prove damages as required under the act. The court found merely accessing the information and using the information while employed for a competitor was not "impairment to the integrity or availability of data, a program, a system, or information." (Sam's Wines & Liquors, Inc v Hartig, 2008)

In the MBTA case the access was to a chip in a card and the MBTA web site. Does the chip in the Charlie card constitute a computer?

**COMPUTER DEFINED**

According to the Computer Fraud and Abuse Act a computer for the purpose of this act was defined as:

> (e) As used in this section--
>
> > (1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
> >
> > (2) the term "protected computer" means a computer--
> >
> > > (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
> > >
> > > (B) which is used in interstate or foreign commerce or communication; (Computer Fraud and Abuse Act , 1986, amended 1986,1994,1996, 2001)

Two critical questions arise that must be answered in the affirmative in order for the Computer Fraud and Abuse Act to be applicable in this case. First, did the CharlieCard and Charlie Ticket fare cards in conjunction with the MBTA system constitute a computer within the meaning the Computer Fraud and Abuse Act? Secondly, if the MBTA system is, in fact, a computer, is it a protected computer?

Addressing the first question of whether the ticketing system is a computer, it is certainly an electronic system that also includes magnetic features embedded within the access cards. The fare data is processed employing devices that arithmetically calculate the proper fare and operate using logic and memory to store information regarding fares and credits purchased to be applied to fares charged as the MBTA transportation system is accessed. Certainly the CharlieCards and Charlie Tickets operating in conjunction with the fare system were devices used to both store fare and credit information and communicate with the MBTA computing and data processing system that controlled access of riders to the transportation system.

Secondly, did this computer system qualify as a protected computer within the meaning of the statute? The Computer Fraud and Abuse Act is designed to protect computer systems of the United States government, financial institutions, or any computer used in interstate or foreign commerce or communication. Since the MBTA system was neither a financial computer system or a U.S. government computer system, in order for the Computer Fraud and Abuse Act to apply jurisdictionally to this case, the MBTA computer system must be one “which is used in interstate or foreign commerce or communications.” The MBTA computer system is used in interstate commerce in that the CharlieCards and Charlie Tickets are routinely sold and value added to them over the Internet, which makes the system accessible directly via interstate commerce. Fraudulent use of a stored value card such as the CharlieCard can impact interstate commerce.

In the MIT case it clear that the students violated the authorized used of the MBTA’s computers as defined by the Computer Fraud and Abuse Act. Almost all the cases in which courts have found a violation of the Computer Fraud and Abuse Act was because the plaintiffs failed to meet the $5,000 threshold or did not damage the computer as defined by the act. In an early case, EF Cultural Travel BV v Explora the court found that damages could simply be the cost of a forensic expert to establish the case. (EF Cultural Travel BV v Explora, 2001)

Damages have been interpreted as more than just $5,000 in monetary damages by a few courts. In a 2008 case the court found that the plaintiff must prove damage to the computer system or interruption

to a computer service. That is a minority opinion but in this case the defendants admitted using the system for free rides on a few occasions. (Massachusetts Bay Transportation, 2008)

## WHITE HAT EXCEPTION TO THE CFAA?

In the CFAA there is no specific exception to the act for hackers with good intentions. In fact, the code does specifically state it is a violation of this act if a person "having knowingly accessed a computer without authorization or exceeding authorized access." (Computer Fraud and Abuse Act , 1986, amended 1986,1994,1996, 2001)

There is no educational exception to the CFAA, even if the students' actions were motivated purely on research. The students did not approach the MBTA for permission to conduct the research or present their findings to the MBTA.

The students were taking an upper division class at MIT. They were required to take several classes prior to this security class. The university had an ethics code which the students had access to and should have been familiar with.

In addition the Association for Computing Machinery, ethics of professional conduct section 1.2 provides that harm to others must be avoided. "Harm means injury or negative consequences such as loss of property, property damage, or unwanted environmental impacts." (Association for Computing Machinery, 1992)

## FREEDOM OF SPEECH

In addition, the students argued that the restraining order and the possible injunction was a prior restraint of speech and would violate their right to free speech. The First Amendment to the Constitution guarantees free speech and subsequent cases clarified that court will not allow prior restraint of speech unless allow the speech will likely cause imminent lawless action. Brandenburg v. Ohio, 395 U.S. 444 (1969). This is the standard for government prior restraint of speech. In this case, the students were promising to teach others how to ride for the MBTA for life for free. If the students fulfilled that promise through their presentation at Defcon it would have caused significant financial loss to the MBTA. It is very likely that many individuals would have taken the published methods and caused chaos and severe financial loss to the MBTA if informed of how to ride for free. If the students were to incite others to commit crimes, they could face civil and criminal penalties for that action. An injunction against publishing

## INJUNCTIONS

The students were supported by their university, their instructor, Hacker community, Electronic Frontier Foundation and the ALCU. The ALCU said the students should be protected under academic freedom. (Massachusetts Bay Transportation, 2008) Academic freedom is a principle first outlined in a 1940 Supreme Court Case. It refers to the teachers not the students and states specifically, "It is the special task of teachers to foster those habits of open-mindedness and critical inquiry which alone make for responsible citizens, who, in turn, make possible an enlightened and effective public opinion." (Kay v Board of Education, 1940). This case was about students who violated a federal statute and many ethical codes.

Judge Douglas P Woodlock granted the temporary restraining order but Judge O'Toole dismissed the motion for an injunction. Further O'Toole ruled that it was "unlikely that the CFAA would apply to security researchers giving an academic talk," (Massachusetts Bay Transportation, 2008)

Judge O Toole further stated: "A presentation at a security conference is not some sort of computer intrusion. It's protected speech and vital to the free flow of information about computer security vulnerabilities. Silencing researchers does not improve security – the vulnerability was there before the students discovered it and would remain in place regardless of whether the students publicly discussed it or not." (Massachusetts Bay Transportation, 2008)

What the judge does not address is the fact the security breach may have been there before the students found it but most people weren't aware of the breach or if they were aware they wouldn't have know how to breach it. The students were not making a presentation about the fact a breach exist but a how-to seminar.

In addition, it is an important principle of white hat hacking that there be responsible disclosure. The students' lawyers argued that the students met the standard because although they did not voluntarily notify the MBTA they intended to withhold key elements from their talk to cheat the fare collection. However, when the students agreed to present at the Defcon, hacking convention they promised to present the information that would allow "free rides for life."

There is no provision in the Computer Fraud Abuse Act for responsible disclosure. The students also argued that there was other research available that discussed this problem. If that were the case then maybe the students didn't deserve an A for their efforts.

## CRIMINAL ACTS

Although the students claimed this hacking was done merely as a research project, the MBTA was able to show that the students actually used tickets for free subway rides that they did not pay for. The students prepared a presentation entitled "Anatomy of a Subway Hack" and within this presentation they had slides of the CharlieTickets (theLinked Tickets). The MBTA was able to link those tickets to show payments and activities using those linked tickets. It showed those tickets were used but not paid for; therefore the students used the tickets illegally.

Dead Addict, one of DEFCON's organizers said "We simply don't take the law as a moral compass." (Middle America meets the Hackers, 2007)

Eventually MBTA dropped the case in exchange of the students revealing the defects to the MBTA Charlie system.

## CONCLUSION

The students were lucky. They violated both the Computer Fraud and Abuse Act and could have been found guilty of the criminal provisions but also could have been pursued civilly by MBTA. There is no provision for either a white hat or a research exception to the law. If the students were attempting to be white hat hackers they violated the basic principle of notifying the company and gaining permission. The act of presenting this information at a hackers' convention and advertising the presentation as "Free Rides for Life" hardly are the acts of a white hat hacker or a researcher. The students' teacher certainly has a prestigious reputation but it was negligence on the teacher's part not to ensure that the student notified the company before hacking into MBTA system.

## BIBLIOGRAPHY

*Association for Computing Machinery*. (1992, October 16). Retrieved February 11, 2009, from Ethics Code: http://www.acm.org/about/code-of-ethics

Chalk v United States, 840 F.2d 701, 704 (9th Cir. 1988).

Computer Fraud and Abuse Act , 18 U.S.C. 1030 (1986, amended 1986,1994,1996, 2001).

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (United States Code 1984, amended 1994).

Craiglist,Inc.v Bertz, 3.2008cv0566 (California Northern District Court November 5, 2008).

*Defcon Communications Inc*. (2009). Retrieved April 3, 2009, from Defcon 17: http://www.defcon.org/

EF Cultural Travel BV v Explora, 274 F.3d577 (U.S. Court of Appeals 2001).

Facebook, Inc. v Studviz, Ltd et , 5:2008cv03468 (California Northern District Court July 18, 2008).

Federal Rules of Civil Procedure, Rule 65 (2007).

Financial Times Limited v The Blackstone Group, L.P. and John Does 1-100, 12009cv00783 (New York Southern District Court January 28, 2009).

Germain, J. (2004, February 13). *Security.* Retrieved March 3, 2009, from TechNewsWorld All Tech-All the Time: http://www.technewsworld.com/story/32847.html?wlc=1246555664

Kay v Board of Education, 18 N.Y.S. 2d 821,829 (1940).

Massachusetts Bay Transportation, 1:2008cv11364 (Massachusetts District Court August 8, 2008).

Messmer, E. (2007). Black Hat probes hacker exploits. *Network World* , 24(30) 12-13.

Middle America meets the Hackers. (2007). *Forbes* , 2.

MySpace Inc v Optinrealbig.com LLC et al, 2:2007cv00496 (California Central District Court January 19, 2007).

Rivest, R. (2009, February). *Course Information.* Retrieved March 15, 2009, from Network and Computer Security: http://courses.csail.mit.edu/6.857/2009/handouts/H01-course-information.pdf

Sam's Wines & Liquors, Inc v Hartig, North District Ill (WL 4394962 September 24, 2008).

Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 119 F. Supp 2d (W.D. Washington 2000).

Ticketmaster LLC v RMG Technologies Inc et al, 2:2007cv02534 (California Central District Court April 17, 2007).

Wilbanks, L. (2008). When Black Hats Are Really White. *IT Professional Magazine* , 10(5), 64, 63.

Young, R. Z. (2007). Hacking into the Minds of Hackers. *Information Systems Management* , 24(4), 281-287.

Zetter, K. (2008). Three Minutes with Jeff Moss. *PC World* .

# Subscription Information

The Proceedings of Lex Informatica: South Africa Cyberlaw and ICT Conference, is a publication of the Association of Digital Forensics, Security and Law (ADFSL).

The proceedings are published in both print and electronic form under the following ISSN's:

ISSN: 1949-1344 (print)

ISSN: 1949-1336 (online)

Subscription rates for the proceedings are as follows:

| | | | |
|---|---|---|---|
| Institutional | - Print & Online: | $120 | (1 issue) |
| Institutional | - Online: | $95 | (1 issue) |
| Individual | - Print: | $25 | (1 issue) |
| Individual | - Online: | $25 | (1 issue) |

Subscription requests may be made to the ADFSL.

The offices of the Association of Digital Forensics, Security and Law (ADFSL) are at the following address:

Association of Digital Forensics, Security and Law
1642 Horsepen Hills Road
Maidens, Virginia 23102
Tel: +1 804-402-9239
Fax: +1 804-680-3038
E-mail: admin@adfsl.org
Website: http://www.adfsl.org

# Contents