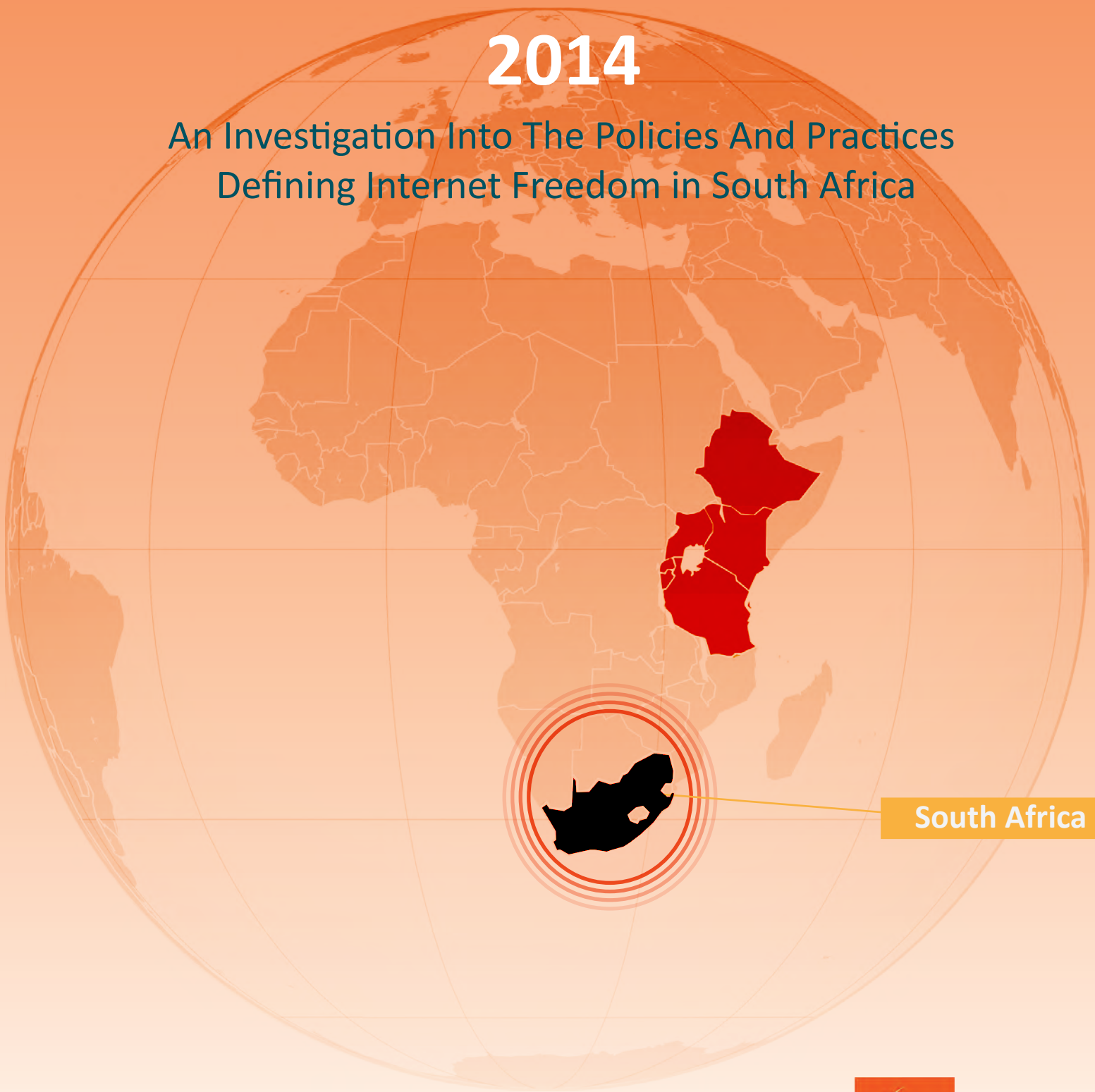
State of Internet Freedoms in South Africa 2014

An Investigation Into The Policies And Practices Defining Internet Freedom in South Africa



OpenNet Africa

CIPESA

Credits

This report was produced by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) in the context of the OpenNet Africa initiative (www.opennetafrica.org) which monitors and promotes internet freedoms in east and southern African countries including Ethiopia, Kenya, Rwanda, Burundi, Tanzania, Uganda and South Africa.

Other country reports have been written for Burundi, Ethiopia, Kenya, Rwanda, Tanzania and Uganda. The country reports, as well as a regional 'State of Internet Freedoms in East Africa' report, are available at www.opennetafrica.org.

The production of this report was supported by the Humanist Institute for Cooperation with Developing Countries (Hivos), the Citizen Lab at the University of Toronto and the Canadian International Development Research Centre (IDRC).

Principal Researcher: Nicolo Zingales, Assistant Professor, Tilburg Law School, Tilburg University, Netherlands.

Contributors: Ashnah Kalemera, Lillian Nalwoga, Juliet Nanfuka, Emilar Vushe and Wairagala Wakabi.

State of Internet Freedoms in South Africa 2014
Published by CIPESA
December 2014

Content

Preamble

This report surveys the state of Internet freedoms in South Africa, including the legal and policy framework, and Internet freedom violations reported to-date. At its core, the notion of Internet freedom gravitated around the idea of freedom of expression and global, unrestricted access to information and ideas. However, a complete picture needs to recognise that certain requisites exist for the flow of information to arise and to unfold undisrupted, namely Internet access, equality, privacy and due process. Thus, in the following sections we will evaluate the extent to which all the essential elements, as well as the central component of freedom of expression, are fulfilled in the current South African legal and policy framework. This is followed by a section revealing the Internet freedom incidents of which we have notice. Finally, we provide recommendations to address some of the shortcomings of the current framework in promoting internet freedom.

Introduction

The use of Information and Communication Technologies (ICT) in South Africa has been on a continuous increase over the last years. It has been estimated that in 2012, 12.3 million South Africans (nearly 41% of the population) had access to the internet, compared to 6.8 million in 2010 and 8.5 million in 2011.[1] [2] By the end of 2013, internet users had increased to 48.9% of the population.[3] However, only an estimated 10% of South Africans have internet access at home; the great majority access from their mobile devices.[4] At the same time, the numbers concerning high-speed internet are promising: South Africa ranks 62nd worldwide for mobile broadband, preceded by just four African countries – Ghana, Zimbabwe, Namibia and Egypt. In contrast, it is significantly worse positioned in terms of individual internet access, where it is ranked 111th worldwide.[5]

Despite the steady rise of internet penetration through mobile technology in the country, fixed-line access continues to decline, largely due to lack of competition in the wholesale market for internet access and an ineffective regulatory environment.[6] The most visible and immediate effect on consumers is higher prices and a lower quality of service in the market for internet connectivity, particularly broadband.[7]

However, a positive step was reached in 2013 through a settlement between the Competition Commission and national formerly state-owned fixed-line operator Telkom. The settlement included pricing commitments and a separation between the company's retail and wholesale divisions, in order to prevent excessive and exclusionary prices to internet service providers (ISPs).[8] The settlement also established continuous monitoring of Telkom's compliance.

The government in 2012 launched the "Strategic Integrated Project 15", designed "to ensure universal service and access to reliable, affordable and secure broadband services by all South Africans, prioritising rural and under-serviced areas and stimulating growth".[9] Further, the National Broadband Policy 2013 approved in December 2013, makes universal service a priority.[10] It also allows for the provision of appropriate support for digital inclusion, the reduction of the costs, the clarification of the role of different stakeholders in the development of broadband, and more generally the formulation of an integrated approach in the deployment of broadband services.

Furthermore, the Minister of Communications issued a call for comments on January 24, 2014 on the National Integrated ICT Policy Green Paper.[11] The paper, which builds upon findings of the Universal Service and Access Agency of South Africa (USAASA)[12], emphasises the importance of programs aimed at enhancing the affordability of computers and smart phones, bringing public access broadband services to smaller towns and villages, and exploring the potential of new technologies to provide telemedicine, smart-metering and telemetry services as part of an expanded universal service.

1 *Statistics South Africa, P0318 - General Household Survey (GHS) 2012, 22 August 2013, http://beta2.statssa.gov.za/?page_id=1854&PPN=P0318&SCH=5598*
2 *Indra De Lanerolle, "The New Wave: Who Connects to the Internet, When they Connect, and What Do They Do When They Connect", Report for the South African Network Society (2012), http://www.networksociety.co.za/internet-report.php*
3 *International Telecommunication Union (2014), Percentage of Individuals using the Internet -South Africa, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls*
4 *World Wide Wox, Executive Summary: Access in South Africa 2012, December 2012, http://www.worldwideworx.com/wp-content/uploads/2012/12/Exec-Summary-Internet-Access-in-SA-2012.pdf.*
5 *ITU & UNESCO, "The State of Broadband 2013: Universalizing Broadband", Report by the Broadband Commission, September 2013, http://www.broadbandcommission.org/documents/bb-annualreport2013.pdf*
6 *Research ICT Africa, "Policy Paper 7 - Understanding what is happening in ICT in South Africa", http://www.researchictafrica.net/docs/Policy%20Paper%207%20-%20Understanding%20what%20is%20happening%20in%20ICT%20in%20South%20Africa.pdf*
7 *Ibid 5*
8 *SAFLI (2013), South Africa: Competition Tribunal, Competition Commission v Telkom SA SOC Ltd (016865) [2013] ZACT 62 (18 July 2013), http://www.saflii.org/za/cases/ZACT/2013/62.html*
9 *Strategic Integrated Project 15, http://www.ellipsis.co.za/strategic-integrated-project-sip-15-expanding-access-to-communication-technology/*
10 *Broadband Policy, 2013, http://www.doc.gov.za/documents-publications/broadband.html?download=90:broadband-policy-gg37119*
11 *Minister of Communications, "National Integrated ICT Policy Green Paper " (2014), http://www.doc.gov.za/documents-publications/ict-policy-review.html?download=89:gazetted-2014-national-integrated-ict-policy-green-paper,*
12 *USAASA (2013): National Strategy on Universal Services and Access – Consultative Document, http://www.usaasa.org.za/export/sites/usaasa/resource-centre/download-centre/downloads/Consultative-Document-on-National-Strategy-signed.pdf*

However, so far there is little track of government-funded programs designed to achieve these objectives, or to increase the use of ICT more generally. Although the government established telecenters (places providing connectivity and access to information via a range of technologies including phone, fax, computers and the Internet in the late 1990s under the Universal Access Fund, the effectiveness and the methodology for their implementation have been criticised.[13] A combination of technical problems, managerial weaknesses and financial difficulties - due in particular to the lack of correlation between the services offered and the demands of the community - have been noted.[14]

The Universal Service and Access Fund (USAF)[15] managed by USAASA finances projects and programs that strive to achieve universal service and access to ICT by all South African citizens. The fund requires every service provider granted a license under the Electronic Communications and Transactions (ECTA) Act 2002[16] to make a mandatory contribution of 0.2% of their annual turnover derived from licensed activity to the USAF. In turn, these payments are used to provide subsidies for: assistance of needy persons to access and use broadcasting and electronic communications services, and financing the construction or extension of electronic communications networks in under-serviced areas. The subsidies are also used for procuring ICT services and for training and payment of allowances to personnel of centres where access to electronic communications networks can be obtained. In 2013, USAASA reported that 104 fully functional access centres out of 120 centres planned under the Rapid Deployment of New Access Centres had been established, and 98 centres received connectivity upgrade out of the 114 centers under the Electronic Communications Infrastructure program.

In 2007, the South African National Research Network (SANReN) was initiated.[17] The project, funded by the Department of Science and Technology (DST), currently provides a minimum of 1Gbps and up to 10Gbps redundant connectivity to all South African public universities.[18] Together with the Centre for High Performance Computing (CHPC) and the Very Large Databases (VLDB) project, SANReN aims to provide South Africa with the key infrastructure for global knowledge production. However, the lack of effective implementation appears to have affected the success of this vision. Initiated in 2009, the VLDB project was designed "to build the infrastructure and skills necessary to cope with the data explosion as a result of the data-driven research initiative". However, the project is still in its first phase, lagging behind with respect to its original target of completion in 2012.[19]

[13] *Attwood, H., Diga, K., Braathen, E. and May, J. "Telecentre Functionality in South Africa: Re-Enabling The Community ICT Access Environment" The Journal of Community Informatics, Vol 9, No 4 (2013)*
[14] *Ibid 14.*
[15] *Universal Service Fund, http://www.usaasa.org.za/usaif/index.html*
[16] *Electronic Communications and Transactions Act (ECA) of 2002, http://www.acts.co.za/electronic-communications-and-transactions-act-2002/*
[17] *South African National Research Network, http://www.sanren.ac.za/*
[18] *Refers to high quality connectivity. It means that the Internet traffic can continue to flow smoothly even if one single point in your connection were to be malfunctioning*
[19] *Council for Scientific and Industrial Research Overview: Cyber infrastructure (2011), http://www.csir.co.za/meraka/cyberinfrastructure/*

Relevant Agencies

Independent Communications Authority of South Africa (ICASA)[20]

The Independent Communications Authority of South Africa (ICASA) is the regulator for the South African communications, broadcasting and postal services sector. ICASA was established by the Independent Communications Authority of South Africa Act of 2000 amended in 2005.[21] ICASA's mandate is spelt out in the Electronic Communications Act, 2005 for the licensing and regulation of electronic communications and broadcasting services, and by the Postal Services Act, 1998 for the regulation of the postal sectors. ICASA also monitors licensee compliance with license terms and conditions, develops regulations for the three sectors, plans and manages the radio frequency spectrum as well as protects consumers of these services.

Department of Communications[22]

The Department of Communications (DoC) aims to develop ICT policies and legislations that create favourable conditions for accelerated and shared sustainable growth for the South African economy. The DoC's mission is to create a vibrant ICT sector that ensures that all South Africans have access to robust, reliable, affordable and secure ICT services in order to advance socio-economic development goals and support the Africa agenda and contribute to building a better world. With Proclamation, No. 47 of July 15, 2014, the South African President Jacob Zuma established a new ministerial function and thereby divided the Department into two units: the Department of Communications and the Department of Telecommunications and Postal Services.[23]

Universal Service and Access Agency of South Africa (USAASA)[24]

The Universal Service and Access Agency of South Africa was established under the Electronic Communications Act (ECA), 2002 with a sole mandate to promote the goals of universal access and universal service. Among others, the agency's strategic objectives include; to make ICT's available, accessible and affordable to all South Africans through the provision of funding from USAF, in collaboration with ICT stakeholders; to undertake continuous research to promote, encourage, facilitate and offer guidance regarding Universal Service and Access, with a view to inform policy and regulatory processes; and to monitor and evaluate the extent to which Universal Service and Access have been achieved in order to assess the impact of the ECA in this regard.

Internet Service Providers Association (ISPA)[25]

The ISPA is an independent body and voluntary association formed in 1996 to deal with the interests of internet access providers in South Africa. The association currently facilitates exchange between the different independent internet service providers, the Department of Communications, ICASA, operators and other service providers in South Africa. As of December 2014, the association had 175 members.[26]

National Broadband Council

The Council, established in March 2014[27], is an independent multi-stakeholder advisory group of technical experts and representatives of business, trade unions and civil society designed to advise the Minister of Communication on the roadmap for broadband development and other policy issues emerging in this fast-changing environment.[28]

[20] *Independent Communications Authority of South Africa, https://www.icasa.org.za/*
[21] *Independent Communications Authority of South Africa Act of 2000, http://www.doc.gov.za/documents-publications/acts.html?download=30:icasa-act-2000*
[22] *Department of Communications, http://www.doc.gov.za/*
[23] *Department of Telecommunications and Postal Services, South Africa: http://www.dtps.gov.za/*
[24] *Universal Service and Access Agency of South Africa, http://www.usaasa.org.za/about/strategic-overview.html*
[25] *Internet Service Providers Association (ISPA), http://ispa.org.za/*
[26] *ISPA – List of Members, http://ispa.org.za/membership/list-of-members/*
[27] *See Ministry of Communications, South Africa Connect: Creating Opportunities, Ensuring Inclusion. South Africa's Broadband Policy (December 6, 2013), http://www.researchictafrica.net/countries/south_africa/South_Africa_Broadband_Policy_-_2013.pdf*
[28] *South Africa launches National Broadband Council, IT News Africa (March 5, 2014) http://www.itnewsafrica.com/2014/03/-south-africa-launches-national-broadband-council/*

Legal and Regulatory Environment

Equality

Article 1 of the South African Constitution affirms that dignity, equality and advancement of human rights and freedoms are essential values upon which the democratic Republic of South Africa is founded.[29] Accordingly, a particular importance is attributed by the Constitution to the rights contained in Articles 9 and 10, relating to equality and human dignity. Both articles are considered non-derogable rights, even in the conditions of state of emergency identified by Article 37.

For all these reasons, it is appropriate to refer as a preliminary matter to the key role played in the South African legal framework by the concept of equality. Article 9 states: *"Equality includes the full and equal enjoyment of all rights and freedoms […] The state may not unfairly discriminate directly or indirectly against anyone on one or more grounds, including race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth."* The article also extends this obligation to private individuals, and establishes that national legislation must be enacted to prohibit such unfair discrimination, but legislation and other measures may be adopted to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

The State has followed these directions through the adoption of the Promotion of Equality and Prevention of Unfair & Discrimination Act (PEPUDA) of 2000.[30] This Act, which attributes jurisdiction to every magistrate court and high court to serve as "equality courts", incorporates the spirit of Article 9 of the Constitution by prohibiting race, gender and disability-based discrimination, and providing further details on the more general notion of unfair discrimination[31], with the aim to promote both de jure and de facto equality. Furthermore, Section 12 outlaws the dissemination and publication of any information that could be "reasonably construed to demonstrate a clear intention to unfairly discriminate". This Section is subject to the provision that this shall not prevent good faith engagement in artistic creativity, academic and scientific inquiry, fair and accurate reporting in the public's interest or the exercise of freedom of expression in accordance with Section 16 of the Constitution.

The PEPUDA Act addresses "hate speech" by adopting its own definition, and prohibiting the publication, propagation, advocacy or communication of words based on one or more of the prohibited grounds "which could reasonably be construed to demonstrate a clear intention to (a) be hurtful; (b) be harmful or to incite harm; (c) promote or propagate hatred". This is in contrast with the fact that only hate speech based on race, ethnicity, gender or religion is explicitly excluded from the protection afforded by Section 16 of the PEPUDA Act. In other words, the Act dangerously expands the notion of unprotected speech by including speech based on any of the open-ended category of "prohibited grounds".

Furthermore, the Act's definition is not limited to speech that "advocates hatred… and that constitutes incitement to cause harm", but targets any speech that can "reasonably be construed to have a clear intention to be hurtful", which encompasses a far broader range of communications. Not surprisingly,

[29] *South African Constitution, http://www.gov.za/documents/constitution/1996/a108-96.pdf*

[30] *South Africa, Department of Justice and Correctional Services (2000); Promotion of Equality and Prevention of Unfair & Discrimination Act (PEPUDA) of 2000, http://www.justice.gov.za/legislation/acts/2000-004.pdf*

[31] *In particular, focusing on factors such as (a) whether the discrimination impairs or is likely to impair human dignity; (b) the impact or likely impact of the discrimination on the complainant; (c) the position of the complainant in society and whether he or she suffers (d) patterns of disadvantage or belongs to a group that suffers from such patterns of disadvantage; (e) the nature and extent of the discrimination; (f) whether the discrimination is systemic in nature; (g) whether the discrimination has a legitimate purpose; (h) whether and to what extent the discrimination achieves its purpose; (i) whether there are less restrictive and less disadvantageous means to achieve the purpose; and whether and to what extent the respondent has taken such steps as being reasonable in the circumstances to accommodate diversity, or to address the disadvantage which arises from or is related to one or more of the prohibited grounds. See PEPUDA, Section 14.*

the breadth of this provision was recently challenged as unconstitutional. At the time of writing this report, a ruling was yet to be made on the issue.[32]

Freedom of Expression

The right to freedom of expression is enshrined in Section 16 of the Constitution, which includes an illustrative list of concepts that fall within the categories of protected speech: (a) freedom of the press and other media; (b) freedom to receive or impart information or ideas; (c) freedom of artistic creativity; and (d) academic freedom and freedom of scientific research.

The Section also defines three forms of expressions that fall outside the scope of protection: (a) propaganda for war; (b) incitement of imminent violence; and (c) advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm. It is important to note that these categories do not simply provide limitations to the exercise of the right to free speech as set out in Section 16 (1), but define its scope altogether. This is of particular importance insofar as the implementation of legislation in these "excluded areas" does not require the fulfilment of the general test devised by Section 36, according to which: "The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including: (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose."

The test of Section 36- in conjunction with Section 16 (1) - applies to the Film and Publication Act (FPA),[33] a law passed in 1996 with the objective to regulate the creation, production, possession and distribution of films, games and certain publications in order to protect children and consumers in general from exposure to disturbing and harmful material, and to make the use of children in and the exposure of children to pornography punishable. The FPA identifies a number of categories of harmful or potentially harmful material, and creates a regime of registration, classification and authorisation by the Film and Publication Board (FPB)[34], which must be complied with by anyone intending to exhibit, distribute, publish, broadcast or otherwise make available to the public a "publication".

By definition of the FPA, "publication" refers to a wide range of material, such as *"any message or communication, including a visual presentation, placed on any distributed network"*. Although exceptions can be requested for scientific and artistic material, publishing or knowingly distributing or exhibiting a film or game without having registered with the FPB results in the commission of an offence and a liability to a fine or imprisonment for up to six months.

Similarly, making available, importing, creating or possessing (or even facilitating the possession) of child pornographic material constitutes an offence, the only defence to which is that such material is (a) for a bona fide documentary, (b) a publication of scientific, literary or artistic merit, or (c) on a matter of public interest (section 16). This particular provision of the FPB came under scrutiny in De Reuck v. Director of Public Prosecutions[35], where the Constitutional Court found that the prohibition did not restrict expression unjustifiably, primarily because it permits exemptions - although the criteria for being granted such exemptions are unclear.

However, on September 28, 2012, the Constitutional Court evaluated the chilling effects of this authorisation system with regard to publications containing sexual content, and declared the mechanism unconstitutional. Court ruled that the law could have imposed less severe restrictions on

[32] *Sapa, "Qwelane challenges equality law", IOL News, October 2, 2013, http://www.iol.co.za/news/crime-courts/qwelane-challenges-equality-law-1.1586128#.Uv51-3czKXs*

[33] *Film and Publication Act (FPA) 1996, http://www.fpb.org.za/profile-fpb/legislation/doc_download/293-films-and-publications-act-no-65*

[34] *Film and Publication Board, http://www.fpb.org.za/*

[35] *De Reuck v Director of Public Prosecutions (Witwatersrand Local Division) and Others (CCT5/03) [2003] ZACC 19; 2004 (1) SA 406 (CC); 2003 (12) BCLR 1333 (CC) (15 October 2003), http://www.saflii.org/za/cases/ZACC/2003/19.html*

freedom of expression, or simply permitted a publisher to obtain an advisory opinion by the FPB without being penalised for failure to do so.

Another perceived challenge of the FPA Act is that it requires all ISPs (a category which to-date is interpreted to include cyber cafes) to register with the Board, as well as to take all reasonable steps (without clarifying whether this implies deep packet inspection, or shallow packet inspection would be sufficient[36] to prevent the use of their services for the hosting or distribution of child pornography. Despite the identification of an offence and the liability to a fine or imprisonment for up to five years (or both) for failure to comply with such provisions, no constitutional challenge has been made to-date.

Right to Information

The Constitution establishes a "right to information" in Section 32, according to which: "Everyone has the right of access to: (a) any information held by the state, and; (b) any information that is held by another person and that is required for the exercise or protection of any rights". Paragraph 2 of the same section directs the national legislator to enact a law in order to give effect to this right, a provision that was implemented with the enactment of the Promotion of Access to Information Act (PAIA) in 2000.[37]

Not surprisingly, PAIA identifies some limitations to the exercise of this constitutional right of access, in particular the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance. However, it is noteworthy that the Act carves out exemptions for situations that are considered of "public interest", such as: (a) the duty to provide information about the results of any product or environmental testing or other investigation whose disclosure would reveal a serious public safety or environmental risk, (Section 36 [2]), and (b) the duty to grant requests for access if disclosure would reveal evidence of substantial contravention or failure to comply with the law, imminent and serious public safety or environmental risk, or if the public interest in disclosure of the record clearly outweighs the harm contemplated in the provision (sections 46 and 70). These exceptions would de facto legitimise or facilitate the operation of "whistleblowers".

Running counter to this remarkable trend, the National Assembly in late 2011 approved the Protection of State Information Bill[38], which was approved by the upper house of the Parliament. The Bill significantly amends the PAIA 2000 by introducing a regime of classification for "all matters relating to the advancement of the public good" and "the survival of the security of the state". Without providing a clear definition of these terms, the bill imposes substantial penalties (including prison sentences) for publication of classified information. Following criticism from civil society and opposition parties, the National Council of Provinces revised the bill by narrowing the definition of national security, removing from the classification regime all commercial information and introducing a limited public-interest exception.[39] The National Assembly approved this version of the Bill on April 25, 2013[40], but significant mobilisation from civil society led President Jacob Zuma to eventually refuse to sign the bill into law.[41]

Privacy and Data Protection

The right to privacy is explicitly secured by Article 14 of the Constitution. Importantly for the context of ICT communications, the formulation of this Section includes citizens' right *"not to have… (d) the privacy of their communications infringed."* The Constitution did not require any action for the right to

[36] *Both are types of analysis of packets of data that are being exchanged through an ISP's network. While shallow packet inspection limits itself to the packet header, i.e. the information of origin and destination, deep packet inspection also examines payloads, frequency and applies any possible fingerprinting which is deployed based on keywords; Klaus Mochalski, Hendrik Schulze, "Deep Packet Inspection. White Paper. Technology, Applications & Net Neutrality", Ipoque 2009, www.ipoque.com/sites/default/.../white-paper-deep-packet-inspection.pd*

[37] *Promotion of Access to Information Act (PAIA) 2000, http://www.dfa.gov.za/department/accessinfo_act.pdf*

[38] *Protection of State Information Bill, http://www.parliament.gov.za/live/commonrepository/Processed/20111123/384294_1.pdf*

[39] *Freedom House; South Africa Freedom of the Press, 2013 http://www.freedomhouse.org/report/freedom-press/2013/south-africa#.VCBEl2MYVEA*

[40] *BBC News, South Africa 'secrecy bill' approved by parliament, April 23, 2014, http://www.bbc.com/news/world-africa-22298825*

[41] *Smith.D, South Africa secrecy law surprise as Zuma rejects controversial bill, September 12, 2013, http://www.theguardian.com/world/2013/sep/12/south-africa-zuma-secrecy-bill*

privacy to be in effect. In fact, even in the absence of specific implementing or detailing legislation, courts were still obliged by the general provision of Section 8 of the Constitution "when applying the provisions of the Bill of Rights to natural and juristic persons […] to develop the common law to the extent that legislation does not give effect to that right". Thus, in the long period of absence of a specific legislation, the law of privacy was, with the exception of those situations covered by the PAIA from 2000, essentially developed by the courts.

Accordingly, the enactment of comprehensive privacy legislation on November 19, 2013 represents a very significant development in this area. One of the issues clarified by this Protection of Personal Information Act No. 4, 2013 (POPIA)[42] is the fact that personal information may be collected from a source other than the data subject if, among other things, such collection is necessary to avoid prejudice to law enforcement by any public body, in the legitimate interests of national security; or to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied (Section 12 (2) (d)). In the interest of the public, the POPIA allows for authorities to breach privacy rights whenever the public interest, or the benefit to the data subject or a third party derived from the processing, outweighs to a substantial degree any interference with the privacy of the data subject that could result from the processing - (Section 37 (1)). The section is silent on the procedures for obtaining such authorisation from ICASA.

From an institutional perspective, the significant novelty introduced by the POPIA is the figure of an Information Protection Regulator, entrusted with several responsibilities including the monitoring and enforcement of compliance with the Act, the mediation and conciliation of disputes relating to actions in the interest of the protection of personal information, and the occasional issuing of codes of conduct. Unfortunately, this person has not been appointed yet.

Another law affecting the extent of privacy enjoyed by South Africans is the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA)[43], which allows for lawful interception of communications with prior authorisation from a judge. Section 42 outlaws unlawful disclosure of information on the extent of interceptions undertaken pursuant to the provisions of the Act. Under sections 30-31 of the Act, telecommunication service providers are required to provide a service which "has the capability to be intercepted" and to store communication-related information in the modality specified by the license issued by the Department of Communications, at their own expense and for a period of no less than three and no more than five years.

In addition, telecommunications service providers may be required to duplicate signals to an "Interception centre". This could offer the government a significant strategic advantage to prey on targeted users. As provided in the National Key Points Act, if it appears that the loss, damage or disruption or immobilisation of any of these centres may prejudice the Republic, or if it is expedient for the safety of the Republic or the public interest, the Minister of Defence can declare them "national key points". Declaring an area a national key point could trigger application of a strict anti-disclosure regime. This could cause serious repercussions for citizens whereby any person disclosing "any information" in "any manner whatsoever" about security measures can face up to three years in jail or a fine of R 10,000 (US$ 863), without any "public interest" defense being available.[44]

In the spirit of combating terrorism, RICA also contains provisions requiring registration of Sim cards users with identity document numbers and proof of residential address. The Act also requires suppliers of cryptography services to disclose the decryption key or provide decryption assistance upon request of law enforcement, security or intelligence agencies for crime prevention purposes and threats to national security. RICA has no provisions for safeguarding parties whose communications are being decrypted.

42 *Protection of Personal Information Act, http://www.issafrica.org/uploads/SA-POPI-Act-2013.pdf*

43 *Interception of Communications and Provision of Communication-Related Information Act (RICA) of 2002, http://www.justice.gov.za/legislation/acts/2002-070.pdf*

44 *Right2Know, How the National Key Points Act undermines the public's right to know, 4 October 2012, http://www.r2k.org.za/2012/10/04/how-the-national-key-points-act-undermines-the-publics-right-to-know/*

A further significant development with regard to interception was the passing of the General Intelligence Laws Amendment Act, 2013 (GILAA) in July 2013.[45] Despite the withdrawal of the provision of enabling interception of communications from outside of South Africa without judicial warrant – a category vaguely defined as "foreign signals intelligence" - from the previous text of the bill, the Act maintains a sweeping definition of "counter intelligence" and "domestic intelligence" activities. The Act has been criticised for giving 'too much power' to security agencies to monitor citizens' communications.[46]

In its Law Enforcement Disclosure report 2014, Vodafone revealed that governments in some 29 countries in which it operates were requesting its subscribers' data, including without warrants. However, the British company could not disclose the statistics on data requests in South Africa due to provisions in the Regulation on Interception of Communication and Provision of Communication-related Information Act which prohibit the disclosure of the fact that any demand for lawful interception or communications data has been issued by the state.[47]

Intermediary Liability

The South Africa Constitution contains two fundamental provisions on due process applicable to administrative action and court proceedings respectively. Section 33 recognises the right to an administrative action that is lawful, reasonable and procedurally fair, including the right of everyone who has been adversely affected by an administrative action to be given written reasons. The Section further provides that national legislation must be enacted to give effect to these rights, providing among other things for the review of administrative action by a court or, where appropriate, an independent and impartial tribunal. Similarly, Section 34 enshrines the fundamental right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum. Both rights are expression of the principle of fair trial enunciated by Article 10 of the UN Declaration of Human Rights, Article 14 of the International Covenant for Civil and Political Rights, as well as Article 7(1) of the Banjul Charter on Human and Peoples' Rights.

Although it is evident that due process would come up in respect to any dispute relating to the exercise of internet freedom –including all the above - the area where respect of this right is most problematic is that of intermediary liability.

Intermediary liability refers to the attribution of legal responsibility to an ISP for violations committed by its users. "Due process" can be applied to intermediary liability when there is a risk that the illegality of the conduct is determined without ensuring respect for the right of the alleged primary infringer (the user) to be heard. It could also be applied in the event of an automatic imputation to the ISP based on the expectation of a certain degree of oversight over content that would exceed the specific principle set out by the Electronic Communications and Transactions Act (ECTA) of 2002 under Section 78.[48] It could also apply when there is need to identify fault for the attribution of secondary legal responsibility.[49] This usually requires the participation of the ISP by allowing it to make representations, in this sense either in the administrative phase or at the appeal stage. These concerns are well founded in the current framework for Internet intermediary liability in South Africa.[50]

[45] *General Intelligence Laws Amendment Act, 2013, http://www.ssa.gov.za/Portals/0/SSA%20docs/Legislation/GeneralIntelligenceLawsAmendmentAct%20No11of2013.pdf*

[46] *SABC (2013), State security agencies hold too much power: Campaign, Friday 26 July 2013, http://www.sabc.co.za/news/a/819b2200407d29dc84189738b59b7441/State-security-agencies-hold-too-much-power:-Campaign*

[47] *Vodafone Law Enforcement Disclosure Report, http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html#eocp*

[48] *Electronic Communications and Transactions Act 25 of 2002 (ECT Act), http://www.acts.co.za/electronic-communications-and-transactions-act-2002/*

[49] *J. Neethling, J. M. Potgieter& P. J. Visser, LAW OF DELICT, Lexis Nexis 2002*

[50] *A specific application of that principle in the context of copyright law is provided by section 23 (3) of the Copyright Act of 1978, according to which "The copyright in a literary or musical work shall be infringed by any person who permits a place of public entertainment to be used for a performance in public of the work, where the performance constitutes an infringement of the copyright in the work: Provided that this subsection shall not apply in a case where the person permitting the place of public entertainment to be so used was not aware and had no reasonable grounds for suspecting that the performance would be an infringement of the copyright."*

The ECTA (2002) defines an ISP as "any person providing information system services"; and in turn, such information system services are "the provisions of connections, the operation of facilities for information systems, the transmission or routing of data messages between or among points specified by the user and the processing and storage of data, at the individual request of the recipient of the service". The Act includes limitations to the liability of ISPs as seen in Chapter 11. However, different from many countries with similar legislation, the South African framework conditions the limitations of liability to two additional requirements: (1) the ISP's membership of an Industry Representative Body (IRB); and (2) and the adoption and implementation of the corresponding code of conduct.[51]

It should be noted that the proportionality of the first requirement is questionable, particularly for small service providers ;[52] as it potentially prevents them from either engaging in conduct (including speech) that may give rise to liability under this Chapter, or from starting the business activity altogether.[53] To-date, only the ISP Association (ISPA) has obtained an Industry Representative Body (IRB) status.

The requirement concerning the "code of conduct" was integrated by the Minister of Communications in 2006 with the issuance of the "Guidelines for recognition of industry representative bodies of information system service providers". By largely reaffirming the "hands off" approach chosen by the legislator, it was stated that "the only monitoring or control done by the State […] is to ensure that the IRB and its ISPs meet certain minimum requirements".[54] Accordingly, the Guidelines lay out such minimum requirements in addition to several "preferred" (that is, non-compulsory) requirements and a number of principles, including fairness and effectiveness. However, it appears that such principles, and in particular that of "fairness" –which refers to "not adversely affect[ing] the economic viability of ISPs" - is contradicted by the actual practice, in light of the complexity of regulations applicable to this business.

For example, one important principle restates the rule laid out in Section 78 of ECTA, where ISPs are not obliged to monitor the data they transmit nor to actively seek facts or circumstances indicating an unlawful activity. However, such principle is not applicable with respect to procedures prescribed by the Minister to report illegal activity or identify users, such as those set out by the FPA on child pornography.[55]

A crucial task of the guidelines is to direct the IRB to define a specific takedown procedure, published on the IRB's website and to which members must provide a link from their websites. The Guidelines indicate that this procedure needs to be in line with the requirement set out by Section 77 (1) of ECTA. This section specifies the particulars a complainant has to provide in order to notify a service provider or its designated agent of unlawful activity (such as location, nature of the infringing material, remedial action required and contact details).

The ISPA Code of Conduct developed to adhere to these ministerial guidelines was formally adopted in 2008.[56] It lists provisions for the respect of freedom of expression, privacy and confidentiality of internet users, consumer protection and provision of information to customers; availability of standard terms and conditions to customers, dealing with unsolicited communications ("spam"); prevention of cybercrime; protection of minors; lawful conduct; awareness of unlawful content and

[51] *Section 71 clarifies that such recognition can only be obtained upon request to the Minister, provided that he is satisfied that the members of the representative body under examination are subject to a code of conduct; that membership is subject to adequate criteria; that the code requires continued adherence to adequate standards of conduct, and that the representative body is capable of monitoring and enforcing the code of conduct adequately.*

[52] *Alex Comninos, "Intermediary liability in South Africa", Intermediary Liability in Africa Research Papers, No. 3, Association for Progressive Communications (2012), http://www.apc.org/fr/system/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf*

[53] *Fees for membership of ISPA- the only IRB in SA are not negligible, amounting to a minimum of a monthly fee R525 (USD 46) + R73.5 (USD 6.4) VAT for small/affiliate ISPs. See http://ispa.org.za/membership/*

[54] *Minister of Communications in 2006 Guideline, Part 1 &2*

[55] *However, it needs to be specified that ECTA has wider coverage than the FPB, whose definition of an ISP as "any person whose business is to provide access to the Internet by any means" is applicable only to the category of Internet Access Providers (IAPs).*

[56] *ISPA, Code of Conduct, http://ispa.org.za/code-of-conduct/*

activity under which members must establish a notification and takedown procedure for unlawful content and the ISPA's takedown procedure.

However, the guidelines leave arguably excessive discretion for IRBs in the design of such procedure, resulting in the lack of certainty over the effective fulfilment of the requirements of ECTA. For example, they list requirements concerning the observance of consumer protection and privacy provisions of ECTA merely as optional "preferred requirements", as provided in sections 6.5 and 6.6. This is in contrast to the explicit word "obligations" provided by Chapter 7 and 8 of ECTA, Chapter 2 of RICA and 3, 4 and 5 of PAIA.

Indeed, Section 79 of ECTA makes clear that liability limitations provided for by Chapter 11 of ECTA do not affect "any obligations founded on an agreement, licensing and regulatory obligations, and any court or legal obligations to remove, block or deny access to data messages". This implies that ISPs will still be liable for failure to remove or wrongful takedown of unreasonably discriminatory and indecent content. On the positive side, this provision could lead to the legitimisation of stricter liability regimes not only for the strengthening of ISPs or fighting defamatory speech, but also for the protection of human rights in the provision of services. At the same time, however, according to (Section 79 (d)) of ECTA Act, this regime must not interfere with "any right to limitation of liability based on the common law or the Constitution".

Further, the absence of detailed provisions in the Guidelines creates a situation where ISPs are not free to establish any "notice" or "notice and put-back" mechanism, which would allow the user to respond to the allegations of infringement or, respectively, to provisionally restore the allegedly infringing content. In fact, the Internet Service Providers Association (ISPA) has refrained from inserting such safeguard mechanism in its takedown procedure.[57] This issue was brought under the spotlight with proposed amendments to the ECTA 2002. The ECTA Amendment Bill of 2012[58] introduces section 77A, entitled "Right to remedy on receipt of a take-down notice". The section aims to allow for the right of reply in accordance with the principles of administrative justice and the *"audi alteram partem"* (hear the other side too) rule.

However, the mechanism by which it proposes to do so is equally inadequate. The section merely requests ISPs to respond to a "first take-down notice" within 10 business days (or less, if the complainant can demonstrate irreparable or substantial harm), as opposed to informing the concerned user and allowing him to intervene in the process by making representations in his defense.

Furthermore, the proposed amendment does not foresee any kind of liability on the ISP for failure to respond to such notice. Rather it establishes ISP liability only in case of failure to implement a "final take-down notice". That is a notice that a complainant is entitled to issue if (a) after due consideration of the response by the ISP, he considers that the matter has not been resolved to his satisfaction; or (b) he has received no response from the ISP within the allotted time period. Therefore, even with the eventual passing of the proposed amendments to the ECTA, ultimately the complainant decides whether something should be removed by the ISP, much to the dismay of the principle of due process.

Indeed, the genuineness of the adversarial process which the amendment tries to introduce by calling for the intervention of ISPs is bound to be undermined by the misalignment of the interest of the users with those of ISPs. This is the case for two reasons: first, for concerns about potential liability of ISPs for failure to remove content; second, because of the administrative and economic burden that defending the case of their users entails. The potential risk of abuse of the notice and takedown procedure is only in part attenuated through Section 77 (2) of ECTA. This section establishes liability for wilful misrepresentation. Lamentably, it is not clear what amounts to "wilful", namely whether mere

[57] *See ISPA, Take Down Procedure v. 3.2, http://ispa.org.za/code-of-conduct/take-down-procedure/*
[58] *Electronic communications and Transactions Amendment Bill; http://us-cdn.creamermedia.co.za/assets/articles/attachments/42287_n888.pdf*

negligence of the complainant would be sufficient for the application of the provision. Finally, the envisaged procedure provides no mechanisms of appeal before an independent body, which constitutes a core right enshrined in the Constitution.

A brief overview of the categories identified by Chapter 11 of ECTA 2002 also reveals significant divergence from standard international practice. This is not the case for Section 73, which offers a traditional "mere conduit" safe harbour for ISPs. It stipulates that an ISP "is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control" where it fulfils the following conditions of "non-interference" with the communication: (a) does not initiate the transmission; (b) does not select the addressee; (c) performs the functions in an automatic, technical manner without selection of the data; and (d) does not modify the data contained in the transmission.

Similarly, Section 74 provides a standard scope of protection for "caching", exempting ISPs from liability for "the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request".

Section 75 of the ECTA 2002 Act provides for "hosting". It states that a service provider is not liable for damages arising from data stored at the request of the recipient of the service, as long as it (a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or (b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and (c) upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.

Given the specific type of procedure required to complain by sections 74 and 75, it is not clear what would happen if a notification did not follow such procedure, and were nonetheless sufficient to generate actual or constructive knowledge on the provider. Conceivably, this would be enough to lead to liability under traditional common law standards. For example, in the field of copyright, South African courts have defended the idea that indirect liability is triggered when a copyright owner suffers an economic loss that was foreseeable by a defendant who was under a legal duty to prevent it.[59] The courts have rejected defences grounded on pleaded ignorance over the illegality of the works being distributed through the services of the ISP [60] ; finding sufficient the notice of facts that would suggest to a reasonable person that a copyright infringement was being committed; [61] or simply that an inquiry should have been done into whether copyright subsisted or not.[62]

Finally, section 76 of ECTA exempts ISPs from damages for the provision of a category of services consisting of referrals or links to a web page containing an infringing data message or infringing activity by using "information location tools", including a directory, index, reference, pointer, or hyperlink. The section repeats the exact same conditions laid out for "host" providers, except for the fact that the obligation of removal upon notification does not refer to the takedown procedure of section 77, but to a more generic "being informed" - which obviously raises a question in terms of what is appropriate to that end.

In addition, this section contains a further condition requiring the ISP not to receive a "financial benefit directly attributable to the infringing activity". This may be problematic insofar as the incremental revenue for advertising – the main financial source for providers of information location tools - could be considered sufficient to exclude a provider from the liability limitation altogether. In practice, this would require ISPs to screen any type of content in connection with what they are advertising, a task

[59] *Arthur E Abrahams & Gross v Cohen and others, 1991 (2) SA 301*
[60] *Frank & Hirsch (Pty) Ltd v A Roopanand Brothers (Pty) Ltd, 1991 (3) SA 240, at 467*
[61] *Gramophone Co Ltd v Musi Machine (Pty) Ltd and others, 1973 (3) SA 188,at 188; Paramount Pictures Corporation v Video Parktown North (Pty) Ltd, 1986 (2) SA 623 (T), at 251*
[62] *Frank & Hirsch (Pty) Ltd v A Roopanand Brothers (Pty) Ltd, 1991 (3) SA 240, at 467*

that can be as burdensome as requiring ISPs to monitor any information that they transmit – in plain contrast with the spirit of section 78.

Overall, the regime just described only appears to confer the ISPs substantial immunity from liability for the content produced by their users. However, this regime unfortunately fails to provide this much needed security, both because of its limited scope and lack of clarity regarding some of its provisions. First of all, unlike many other regimes around the globe, ISPs may be subject to injunctions, as well as liable under criminal law, for the conduct of their users. Second, the immunity from liability does not apply horizontally across the board, but explicitly carves out different modes of liability under specific legislations such as FPA, RICA or the Equality Act.

Further, the immunity conferred is deficient as ISPs could still be found liable if the knowledge gathered outside the notice and takedown procedure were considered sufficient to meet the standards of liability under common law. This inconsistency generates a rule of law problem as the law is not sufficiently clear and does not enable ISPs to make informed decisions. Additionally, the legal framework adopted conflicts with due process as it permits the establishment of a violation without ensuring full respect of the right to be heard of the accused infringers.

Incidents of threats to Internet freedom

This section captures the major censorship or surveillance incidents that have occurred or are suspected to have occurred in recent years. Reporting these kinds of incidents can give anecdotal evidence and potentially show, depending on their frequency and magnitude, that the flaws and deficiencies in the current laws and policies have serious significance.

One famous incident of censorship, although only to a limited extent affecting freedom of expression in the digital sphere, concerned a painting called "The Spear" depicting President Jacob Zuma in Soviet attire and with his genitals exposed. The painting was exhibited publicly in May 2012 at the Goodman Gallery in Johannesburg.[63] The painting was also published by the City Press newspaper both in print and online. However, President Zuma and the African National Congress Party obtained an injunction aimed at preventing further display at the museum and by the City Press newspaper. They claimed that it was of pornographic nature and not fit for viewers under 16 years of age as classified by the Film and Publication Board (FPB).[64]

However, the Goodman Gallery appealed the ruling[65] in July 2012 and managed to obtain a reversal by the Film and Publication Board's Appeal Tribunal in August 2012.[66] This case highlights the potential of the classification process being used for censorship purposes. It also stands to give a strong signal of independence by the Appeal Tribunal. It should be noted also that President Zuma himself sought several times to control public discussions including online that concerned him through legal action.[67] Earlier in 2008, it was reported that he had initiated 14 lawsuits for defamation since the beginning of his rape trial in 2006.[68]

Another notable incident showed the great ability of South African civil society to get together and organise itself in reaction to potential threats to their liberties. This was seen in the mobilisation occurring around the possible signature by the President of the Protection of State Information Bill

63 *Global Post, Jacob Zuma 'The Spear' painting removed in deal between ANC, Goodman Gallery, Global Post, 30 May 2012, http://www.global-post.com/dispatch/news/regions/africa/south-africa/120530/zuma-the-spear-painting-removed-anc-deal-goodman-ga*

64 *FPB Classification Of 'The Spear' Artwork, http://cdn.24.co.za/files/Cms/General/d/1940/83d2e76c62e442cab9ec9cfdbaef697d.pdf*

65 *Wet.P (2012), 'The Spear' returns as gallery takes on classification, http://mg.co.za/article/2012-07-10-the-spear-returns-as-gal-lery-takes-on-classification,*

66 *FBA (2012), The Spear Award, Before the Film and Publication Appeal Tribunal, http://www.fpb.org.za/classifications/appeals-tribunal/ap-peals-tribunal-awards/doc_download/234-the-spear*

67 *See: Zapiro (2008), Jacob Zuma and Lady Justice, http://www.zapiro.com/Slideshows/Lady-Justice-Jacob-Zuma; Mail and Guardian (2008), Zuma goes after Rapport – again, January 17, 2008, http://mg.co.za/article/2008-01-17-zuma-goes-after-rapport-again*

68 *Janeth Smith, "Zuma exacts defamation action on media", Iolnews, December 19th, 2008, http://www.iol.co.za/news/politics/zuma-exacts-defa-mation-action-on-media-1.429327#.Uv6WunczKXs*

(also known as "Secrecy Bill") in May 2013, driven by a petition of over 70,000 signatures, of which 50,000 were received in less than 48 hours.[69]

Similarly in February 2013, in the case of General Intelligence Laws Amendment Bill (GILAB), also known as the "Spy Bill", civil society efforts led to a revision of the Bill removing the ability for security and intelligence agencies to intercept without warrant any electronic communication passing through foreign servers.[70]

However, despite these mass reactions, the government retains a wide range of tools and powers to engage in surveillance and censorship. An illustration of the former phenomenon is the discovery in April 2013 by Citizen Lab of two FinFisher command and control servers on the network of the former state monopolist Telkom. However, it was not ascertained whether those servers had actually been put into use.[71]

Meanwhile, there has been a significant increase in the number of requests for removal of content received by Google for alleged defamatory or "hate speech" reasons, which surged from zero in 2011 to three in the first half of 2012[72] and six by mid-year 2013.[73] In the first half of 2013, Google reported a request from the Counter Intelligence Agency for the removal of a blog post that allegedly infringed copyright by criticising a media release that the agency had issued for copyright reasons.[74] The request was denied.

The government of South Africa also made data requests for user accounts to Google – two between July and December 2013 and seven for the period January – June 2014. No data was produced by Google for all nine requests.[75]

In the first half of 2013, Facebook reported 14 requests received from the SA government, with nine requests made on users of the network.[76] The second half of 2013 saw three requests made to Facebook targeting four user accounts.[77] For the period January – June 2014, the country made two requests to the social networking site, relating to one user account. All requests were denied. From the above Google statistics, defamation and indecent speech legislation would appear to be a greater problem for freedom of expression than is copyright. However, one should not forget that these reports only give a partial account, not providing statistics for requests received by private individuals or corporations - the most common scenario in the copyright context.

In fact, data collected by the Internet Service Providers Association (ISPA) from 2009 to 2012 indicates that copyright or trademark infringement constitutes the predominant basis (68%) for takedown requests directed to the association, compared to a much smaller percentage (16%) for hate speech, defamation, privacy and harassment.[78] However, these numbers may also simply reflect an increased awareness of the takedown procedure (which has been used almost three times as much in 2012 as in 2009) by copyright owners – particularly big content producers – than for alleged victims of defamation.

In December 2013, government officials are reported to have arrested an individual allegedly responsible for having uploaded to the Private Bay a "high profile" local movie that had not been released yet.[79]

69 *Avaaz (2013), Zuma: Don't Sign the Secrecy Bill! http://www.avaaz.org/en/zumas_secret_loc/*
70 *RTI (2013), The GILAB (aka the Spy Bill) is back in Parliament – what you need to know http://www.r2k.org.za/2013/02/11/gi-lab-spy-bill-back-in-parliament/*
71 *Freedom House (2013)*
72 *Google (2013), Transparency report, January – June 2012, http://www.google.com/transparencyreport/removals/government/ZA/?p=2012-12*
73 *Google, Transparency Report, Content Removal Requests by Governments, South Africa (2013), http://www.google.com/transparencyreport/removals/government/ZA/*
74 *Ibid 68*
75 *Google Transparency Report, Requests for User Information, South Africa, http://www.google.com/transparencyreport/userdatarequests/ZA/*
76 *Facebook (2013), Government requests report - South Africa Requests for Data January – June 2013, https://govtrequests.facebook.com/country/-South%20Africa/2013-H1/*
77 *Facebook (2013), Government requests report - South Africa Requests for Data July – December 2013, https://govtrequests.facebook.com/country/South%20Africa/2013-H2/*
78 *ISPA, Presentation at the APC/Google workshop on intermediary liability, Johannesburg 10-11 February 2014 (on file with the author)*
79 *Torrent freak, South African Pirate Bay User Arrested For Sharing High Profile Local Movie, 13 December 2013, http://torrentfreak.com/south-african-pirate-bay-user-arrested-for-sharing-high-profile-local-movie-131213/*

Conclusions and recommendations

Surveying the existing legal and policy framework and the reported battles over freedom of expression in South Africa, it is evident that it is a dynamic environment with numerous reforms being proposed and very active participation of the civil society in the debate. The most significant issues that the country is confronted with are of four types: access, freedom of expression, privacy and due process.

In terms of access, the continuing increases of prices and reduction of use of fixed-line broadband calls for intervention by the government to promote competition and universal service. The settlement agreement with the national telecom operator and the publication of the National Broadband Policy and the National Integrated ICT Green Paper are very positive signs, but it is of utmost importance to continue monitoring the achievement of the declared objectives in order to avoid the repetition of past mistakes.

South Africa also needs to review most of the legislation which have actual or potential chilling effects to internet freedoms. This calls for more transparency, awareness, and stimulation of a public debate leading to tackling those fundamental issues through law reform. Incriminating provisions such as those provided under the Equality Act, as well as the reach of the obligation of registration with the Film and Publishing Board and of the incriminating provisions of the Films and Publications Act, need the most immediate revision.

On the privacy side, legislation that provides chilling effects generated by the lack of a constitutional challenge over the extent to which ISPs are required to inspect the content distributed through their networks needs to be amended. This also applies to procedures by which cryptography providers are obliged to surrender their users' information to the authorities in the absence of corresponding safeguards; and the existence of a real necessity for obliging ISPs to retain information of the communications of their users for a minimum period of three years.

Finally, the issue of rule of law and due process comes to the fore with regard to the absence of adequate safeguards in the adjudication of disputes over content involving an ISP. Therefore, legislation on intermediary liability ought to be amended to provide:

(1) Protection from criminal liability as well as injunctive relief ,[80] or at least from a certain type of injunctive relief (as it is the case in the US Digital Millennium Copyright Act);

(2) A clarification concerning the interaction of the safe harbor provisions of the ECTA with other types of obligations applicable to ISPs;

(3) A better definition of the concept of knowledge of illegality, and a clarification that the safe harbor does cover also situations of liability under the common law; and

(4) A significant improvement of the adversarial process of users in the determination of the legality of their actions, requiring their participation in the process of adjudication and the entrustment of the decision to an impartial and independent entity, at the very least on appeal.

[80] *Injunctive relief is when you can obtain an order before a judge to order a party to do or not do something. It can be either preliminary (pending action on the merit) or permanent. See paper http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2536829*

This report was produced by the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) under the OpenNet Africa initiative (www.opennetafrica.org) which monitors and promotes internet freedoms in a number of African countries including Ethiopia, Kenya, Rwanda, Burundi, Tanzania, Uganda and South Africa. As part of the project, we are documenting internet rights violations, reviewing cyber security policies and how they affect internet freedoms, promoting information availability and conducting awareness-raising.

The production of this report was supported by the Humanist Institute for Co-operation with Developing Countries (Hivos), the Citizen Lab at the University of Toronto and the Canadian International Development Research Centre (IDRC).

Collaboration on International ICT Policy in East and Southern Africa (CIPESA)
156-158 Mutesa II Road, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org