SPECIAL EDITION

GLOBAL INFORMATION SOCIETY WATCH 2011 UPDATE I

INTERNET RIGHTS AND DEMOCRATISATION

Focus on freedom of expression and association online

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Global Information Society Watch

2011 UPDATE I

APC HIVOS

Internet rights are human rights team
Joy Liddicoat
Shawna Finnegan
Frederic Dubois
Valeria Betancourt
Anriette Esterhuysen
Jennifer Radloff

Editor
Alan Finlay

Proofreader
Grady Johnson and Soledad Bervejillo

Publication production
Flavia Fascendini

Cover illustration
Matías Bervejillo

Graphic design
MONOCROMO
info@monocromo.com.uy
Phone: +598 2 400 1685

Global Information Society Watch 2011 UPDATE I
Published by the Association for Progressive Communications (APC) and the Humanist Institute for Cooperation with Developing Countries (Hivos)

South Africa
2012

APC-201209-CIPP-R-EN-DIGITAL-164
ISBN: 978-92-95096-73-8

APC and Hivos would like to thank the Swedish International Cooperation Agency (Sida) for its support for Global Information Society Watch 2011 UPDATE I.

MONITORING AND DEFENDING FREEDOM OF EXPRESSION AND PRIVACY ON THE INTERNET IN SOUTH AFRICA

Jane Duncan
Highway Africa Chair of Media and Information Society, School of Journalism and Media Studies, Rhodes University

In 1994, South Africa experienced a largely peaceful transition to democracy after decades of apartheid. This transition also led to constitutional guarantees for fundamental human rights, including the rights to freedom of expression and privacy – rights that are central to internet freedom. While freedom of expression has been largely respected, in the past few years, South Africa's media freedom rating has been downgraded by several international media freedom monitoring organisations, such as Reporters Without Borders (RWB) and Freedom House. Local media and civil society organisations such as the South African National Editors' Forum (SANEF) and the Right 2 Know Campaign (R2K) have expressed concern about a growing trend towards securitisation of the state and attempts to censor critics. Against this backdrop, this report will assess the extent to which the rights to freedom of expression, association and privacy are enjoyed on the internet in South Africa.

Background

This section examines the socio-economic challenges South Africa is facing eighteen years into democracy and will set the context for the rest of the report. A final Constitution, drafted by a Constitutional Assembly consisting of the major political parties, was adopted in 1996, and this Constitution has set the legal framework for transformation in the country. The new constitutional order also replaced parliamentary sovereignty with constitutional sovereignty, presided over by an independent Constitutional Court. The Constitution recognises first, second and third generation rights, although the majority of cases heard by the court have been in relation to first and second generation rights.[1] There is no hierarchy of rights, and each right has to be interpreted on a case by case basis, especially when it comes into conflict with other rights. Furthermore, most rights are not absolute, and are subject to a general limitations clause.

South Africa still faces significant development challenges, especially in the wake of the 2009 global recession which has made it even more difficult to reverse entrenched structural inequalities inherited from apartheid and to create sustainable jobs. According to the Presidency's development indicators for 2010,[2] most of the country's main economic indicators have declined markedly since the start of the 2009 global recession, with the exception of inflation and interest rates. South Africa's ranking in the knowledge economy index has slipped gradually from 49th in 1995 to 65th in 2009, which it attributes to low university through-put, slow internet penetration and decreasing funding for research and development.[3]

Unemployment is in long-term decline, although it remains exceedingly high at 25.3% of the economically active population according to the narrow definition of unemployment and 35.9% according to the expanded definition of unemployment (which includes discouraged work-seekers). The problem has been exacerbated by the global recession. The largest number of unemployed people falls within the 15-34 age group, and unemployed men outnumber unemployed women.[4] Poverty has been alleviated by the introduction of social grants, but inequality remains extremely high, with 70% of income accruing to the richest 20%, while the poorest 10% earn a mere 0.6% of income.[5] Modest gains have been made in increasing access to formal housing, and the country is

1. Jackie Dugard, Socio Economic Rights Institute, speech at local government workshop, University of the Witwatersrand, 29 July 2011.
2. us-cdn.creamermedia.co.za/assets/articles/attachments/31523_development_indicators2010.pdf
3. South African Presidency, "Development Indicators 2010", 17, www.thepresidency.gov.za/MediaLib/Downloads/Home/Publications/NationalPlanningCommission4/Development%20Indicators2010.pdf
4. Ibid, 22
5. Ibid, 23

well on the way to ensuring universal access to water, but electricity roll-out has slowed down after a large increase in the number of connections between 1994 and 2010.[6]

In spite of significant inroads into addressing service delivery backlogs, the country is also beset by mass discontent at the pace of delivery. Since 2004, South Africa has experienced an upsurge in protest action on issues relating to service delivery, corruption, lack of accountability and labour issues (including salary demands), with the number of what the Ministry of Police refer to as "crowd management" incidents reaching record levels in 2010-2011. Sociologist Peter Alexander has referred to these as a "rebellion of the poor", which he maintains is unparalleled for any other country.[7] Youth under the age of 35 constitute 70% of the population, with 35% of the populatoin under 15.[8] Nearly three million of the 6.7 million youth are disengaged from society's major institutions, and youth discontent has been recognised as a key factor in social unrest. The country's youth make up a large percentage of those engaged in protest action.[9]

In response to rising discontent, there are signs of the government becoming increasingly defensive and intolerant of dissent. In response to what they consider to be growing threats to media freedom, RWB has down-rated South Africa's press freedom from 26th place in 2002 to 43rd place in 2012, and Freedom House has also down-rated South Africa from "free" to "partly free".[10] Furthermore, public protests are often banned on spurious grounds and police violence against protestors has also become more prevalent since the re-introduction of the military ranking system in the police which existed under apartheid (considered a "re-militarisation of the police").[11]

An overview of internet-related human rights in South Africa

This section examines the legal, policy and regulatory environment for internet rights. It sets out current approaches to regulation of access to and content on the internet, and outlines the main policy and regulatory initiatives in support of internet rights, as well as areas where internet freedom is limited. This section also maps who the main players are in relation to internet service provision and internet content.

Relevant constitutional and regulatory provisions

The right to freedom of expression guarantees the right to receive or impart information and ideas, but does not extend constitutional protection to propaganda for war, incitement to imminent violence and hate speech, which is defined as advocacy of hatred on the basis of race, gender, ethnicity or religion and speech that constitutes incitement to cause harm.[12] Access to information is also protected as a stand-alone right in the South African Bill of Rights.[13] The Act that gives effect to this right, including over the internet, is the Promotion of Access to Information Act. A related piece of legislation is the Protected Disclosures Act, which protects whistleblowers from occupational detriment if they disclose confidential company information on certain protected grounds.

The Constitution also includes a provision for an independent broadcasting regulator to regulate broadcasting in the public interest, and provides for several independent institutions to assist Parliament in its role as overseer.[14] Other media regulators include the Film and Publications Board, a statutory body falling under the Ministry of Home Affairs, and the self-regulatory Broadcasting Complaints Commission of South Africa (BCCSA).

Communications services are regulated by the Independent Communications Authority of South Africa (ICASA) according to the Electronic Communications Act (ECA), which was promulgated in 2005 to facilitate convergence. The ECA incorporates a semi-layered approach to licensing, with three layers having been identified: Electronic Communications Services (ECS), Electronic Communications Network

6. Ibid, 30-33
7. Peter Alexander, "A Massive REbellion of the Poor", *Mail and Guardian*, 13 April 2012, mg.co.za/article/2012-04-13-a-massive-rebellion-of-the-poor
8. Statistics South Africa, "Social Profile of Vulnerable Groups in South Africa 2002–2010", www.statssa.gov.za/Publications/Report-03-19-00/Report-03-19-002002.pdf
9. Prim Gower, "Idle Minds, Social Time Bomb", *Mail and Guardian*, 31 July 2009, www.mg.co.za/article/2009-07-31-idle-minds-social-time-bomb
10. "How Others Are Reading Us", *Daily News*, 3 May 2012, www.iol.co.za/dailynews/opinion/how-others-are-readingus-1.1287993
11. "Police Brutality", *Leadership Online*, 19 April 2011, www.leadershiponline.co.za/articles/politics/1261
12. Constitution of the Republic of South Africa No. 108 of 1996, Section 16, www.info.gov.za/documents/constitution/1996/a108-96.pdf
13. Ibid, Section 32
14. Ibid, Section 192

Services (ECNS) and broadcasting.[15] Internet service providers (ISPs) are classified as ECSs and therefore require a licence from ICASA; however the Act does not give ICASA jurisdiction over the content of ECSs. ICASA has regulated the cost of Asymmetric Digital Subscriber Lines (ADSL) since 2007.[16]

Internet connectivity in South Africa

Universality of communications has been a central feature of South African communications policy, law and regulation, and as a result universal service and access obligations have been placed on ECNS licencees in the form of meeting roll-out targets as well as contributing financially to universality. A separate agency was established by the 1996 Telecommunications Act, and subsequently the ECA, to promote universal service and access to ICTs in South Africa, called the Universal Service and Access Agency of South Africa (USAASA). The agency manages the Universal Service and Access Fund, which is funded from a levy on licencees, and is meant to provide subsidies for people in need in order to assist them to access ICTs, finance construction of electronic communications networks in under-serviced areas, and facilitate access to ICTs for schools and other public centres.[17] The ECA also makes provision for the licensing of underserviced area licencees, in order to promote access to ICTs in areas with a teledensity of 5% or less.

Internet connectivity is provided on a fixed line or mobile basis, with fixed-line connectivity (largely through ADSL) being provided by the partially privatised fixed-line telephone parastatal Telkom. In 2006, competition to Telkom was introduced in the form of the fixed-line operator Neotel. There are three main mobile networks, Vodacom, MTN and Cell-C, and other service providers such as Virgin Mobile and 8ta riding on these networks, and all provide wireless 3G broadband access to the internet.[18] In 2009, a state-owned broadband company called Broadband Infraco was established with the objective of promoting affordable access to electronic communications by providing long-distance backhaul connectivity nationally and regionally. The major players have invested in several undersea cables landing in South Africa which have greatly increased the bandwidth capacity in the country.[19]

South Africa's internet user base grew 25% from 6.8 million in 2010 to 8.5 million at the end of 2011, which means that penetration is approaching 20% of the population, but access is unevenly spread across the country. Smartphones are the main drivers of internet access in South Africa. Of the total user base, 7.9 million access the internet on their cellphones, with the majority accessing the internet both on their cellphones and through computers, laptops or tablets.[20] By 2011, 81.8% of the population used a cellphone, with 73.3% of these connecting on a pre-paid basis; the fact that cellphones are nearly ubiquitous happened in spite of, not because of, national policy.[21] Vodacom is the most popular network operator, followed by MTN.[22]

According to Research ICT Africa, by 2007-2008, more women than men owned cellphones, although for every one woman that accessed the internet, two men accessed it. While monthly mobile expenditure constituted 29.3% of monthly disposable income, women spent more of their disposable income than men.[23] More recently, and drawing on MyBroadband statistics, the Internet Society of South Africa has stated that 69% of internet users are male, and 31% female. Most users access the internet at work, and the country's economic hub, Gauteng, boasts the largest proportion of internet connections of any of the provinces. Most internet users fall within the 35-54 age group, which is out of synch with the preponderance of youth in South Africa.[24]

Fixed-line connectivity through ADSL is constrained by the lack of growth of the fixed-line network after an initial period of growth after the

15. Arthur Goldstuck, "Telco Jabberwock is Dead!", *Leader*, 6 September 2008, www.leader.co.za
16. Ryan Hawthorne, "Local Loop Unbundling Versus Encouraging the Growth of Wireless Local Loops: Lessons for South Africa from other Countries", n.d., 1
17. Universal Service and Access Agency of South Africa, "About USAF", www.usaasa.org.za/usaif/index.html
18. Rudolph Muller, "Local Loop Unbundling: What Should Be Achieved?", *MyBroadband.com*, 10 October 2011, mybroadband.co.za/news/telecoms/35608-local-loop-unbundling-what-should-be-achieved.html
19. "South Africa – Fixed Line Market and Infrastructure – Overview and Statistics", *Budde.com*, n.d., www.budde.com.au/Research/South-Africa-Fixed-line-Market-and-Infrastructure-Overview-and-Statistics.html
20. South African Press Association, "Internet Use in SA Growing", 10 May 2012, www.news24.com/SciTech/News/Internet-use-in-SA-growing-20120510#
21. Charlie Lewis, "Achieving Universal Service in South Africa: What Next for Regulation?", paper presented at the International Telecommunications Society Conference, Telecommunications: Ubiquity and Equity in a Broadband Environment, Wellington, New Zealand, 26-28 August 2010, link.wits.ac.za/papers/Lewis-2010-USA-RSA-regulation-ITS-paper.pdf
22. All Media Products Survey, 2007BA – January-December 2011, www.saarf.co.za/amps/cellphone.asp
23. Alison Gillwald, Anne Milek and Christoph Stork, "Gender Assessment of ICT Access and Usage in Africa", Vol. 1, Policy Paper 5, 2010, www.ictworks.org/sites/default/files/uploaded_pics/2009/Gender_Paper_Sept_2010.pdf
24. Internet Society South Africa, "South African Internet Users", 24 October 2011, www.isoc.org.za

1994 transition to democracy.[25] By 2011, South Africa's fixed broadband penetration rate was a mere 1.5%: significantly lower than the Organisation for Economic Co-operation and Development (OECD)'s average broadband penetration rate for OECD countries.[26] This distortion in connectivity makes it more difficult for South African internet users to optimise their usage of the internet for the purposes of accessing information, given that mobile connectivity is generally slower and more limited than fixed-line connectivity. South African ADSL subscribers also have to contend with restrictive caps, with some plans only offering 1GB of data per month, although some service providers have begun to offer uncapped ADSL.

South Africa's ability to connect to both voice and data networks has been marred by high user costs, and the lack of transparency about pricing has allowed operators to continue these practices relatively unchallenged. According to Research ICT Africa, South Africa ranked a dismal 30th out of 46 African countries for prepaid mobile telephone affordability. Poor subscribers are the worst affected by the excessively high prices of prepaid or pay-as-you-go rates, including out-of-bundle costs, as the poor were more likely to access the internet on an out-of bundle basis. Data bundle prices have also been the source of considerable controversy in South Africa, although Blackberry has been particularly successful as it offers data at a relatively affordable flat rate.[27]

Internet-related policies

Recognising the fact that the low broadband penetration rate was going to impact negatively on South Africa, the Department of Communications has also developed a National Broadband Policy, which was gazetted in 2010. It defines broadband as an always available, multimedia capable connection with a download speed of at least 256 kbps, and aims to ensure universal access to broadband by 2019, with household penetration standing at 15% by the same year.[28] The department has also gazetted a Local and Digital Content Development Strategy, which proposed the establishment of a digital content fund and content generation hubs to stimulate the development of local content, and the prioritisation of the following content areas: animation, wild-life, documentaries, games and ring-tones.[29] While the development of the policies has been broadly welcomed, concerns have been raised about the weakness of the Broadband Policy and its relatively low target in terms of download speed,[30] as well as its lack of an implementation plan.[31] Furthermore, the elite nature of media discourses surrounding the policy, which tended to adopt a techno-centric rather than development-centric approach that could have made the issues more accessible, has contributed to the lack of proper public scrutiny of the policy.[32] More decisive targets were, however, set in the ICT Industry Competitiveness and Job Creation Compact, approved in July 2011, which commits to 100% broadband penetration by 2020.[33]

Other laws regulating internet content

Electronic transactions are regulated according to a separate Act, the Electronic Transactions Act of 2002. Importantly for ISPs, the Act provides for the limitation of liability for service providers, providing they are members of an industry representative body recognised by the Department of Communications.[34] The Act also criminalises a range of online crimes (such as hacking and spamming and email bombing) and creates cyber-policing in the form of cyber-inspectors, employed by the Department of Communications, who are given wide-ranging powers to monitor and inspect any website or information system and search premises for evidence of

25. Robert Horwitz and Willie Currie, "Politics, Privatisation and Perversity in South Africa's Telecommunications Reform Programme" in *Media Policy in a Changing Southern Africa: Critical Reflections on Media Reforms in the Global Age*, eds. Dumisani Moyo and Wallace Chuma (Pretoria: Unisa Press, 2010), 11-38
26. Rudolph Muller, "SA Broadband Penetration Rates: How Do We Compare?", *MyBroadband.com*, mybroadband.co.za/news/broadband/29586-sa-boadband-penetration-rates-how-do-wecompare.html
27. Lloyd Gedye, "Broadband Price Drop Expected", *Mail and Guardian*, 6 January 2012, mg.co.za/article/2012-01-06-broadband-price-drop-expected
28. Department of Communications, Broadband Policy for South Africa, Government Gazette No. 33377, 13 July 2010
29. Department of Communications, Local and Digital Content Development Strategy for South Africa, Government Gazette No. 32553, 4 September 2009
30. Association for Progressive Communications, "Analysis of the Broadband Policy of South Africa", October 2010, www.apc.org/en/node/11294
31. Lewis, "Achieving Universal Service", 21
32. Wallace Chigona, Johannes Willem Vergeer, Andile Simphiwe Metfula, "The South African Broadband Policy: In the Eyes of the Media", Info, 14, 4 (2012): 65-77
33. Staff writer, "100% Broadband Penetration in SA by 2020: DoC", *MyBroadband.com*, 31 July 2011, mybroadband.co.za/news/broadband/30550-100-broadband-penetration-in-sa-by-2020-doc.html
34. Government of South Africa, Electronic Communications and Transactions Act, Chapter XI: Limitation of Liability of Service Providers, Act 25 of 2002, www.info.gov.za/view/DownloadFileAction?id=68060

cyber-crime on reasonable cause shown, provided they are in possession of a warrant. Their powers have been criticised as overbroad, creating potential for infringements of the right to privacy, and the system remains open to abuse particularly because South Africa lacks a dedicated law on privacy.[35]

Internet content falls within the regulatory framework of the Film and Publications Board, which was set up in 1996 to replace the apartheid-era Publications Control Board. The Board is a portfolio organisation of the Ministry of Home Affairs. The essential difference between the old Board and the new one is that while the old Board acted as a censorship board, particularly of political content that challenged the legitimacy of the apartheid regime, the new Board is meant to confine its role to content classification, with a very narrow range of content being restricted or even prohibited: hence the Board's motto, "We inform, you choose".[36]

Another law that impacts on internet freedom is the Regulation of the Interception of Communications and Provision of Communication-Related Information Act (ROICA) of 2002. The Act regulates the interception of certain communications, including internet traffic, and makes it illegal for communications to be intercepted except according to the framework set out in the Act, which makes provision for a designated judge to issue interception directions requested by law enforcement officers (in the defence force, the intelligence services or the police) on crime-related or national security grounds. Interception directions will be undertaken by the Office of Interception Centres (OIC).

ROICA makes it illegal to establish communications networks that are not capable of surveillance. It places obligations on communications service providers, including ISPs, to assist the state in the interception of communications. Telecommunications operators and ISPs are required by the law to facilitate interception and monitoring of communications and to store communications-related information at their own expense for not less than three years and not more than five years.[37] Furthermore, all cellphone users are required to register their SIM cards, and provide proof of residential address and identity numbers. ROICA was part of a basket of laws passed in the early 2000s to assist in the global "war against terror". All these acts were hotly contested in Parliament on the grounds that they threatened the rights to privacy and freedom of expression and while many unpopular clauses were amended, they were not completely cured of deficiencies and as a result still continue to evoke controversy.

There are other statutory or common law provisions impacting on internet rights. The Promotion of Equality and Prevention of Unfair Discrimination Act, otherwise known as the "Equality Act", was promulgated in 2000 and prohibits unfair discrimination and harassment. It prohibits hate speech, which is defined as "...speech that is or could be reasonably construed to demonstrate a clear intention to be hurtful, harmful or to incite harm, or promote or propagate hatred".[38] Concerns have been expressed about the constitutionality of this provision as it adopts a broader definition of hate speech than what the constitution allows for, which is likely to open the Act up to constitutional challenge.[39]

The common law of defamation can also impact on online content. Defamation in South Africa is defined as the wrongful and intentional publication of a statement which has the effect of injuring a person's reputation.[40] Apartheid-era defamation law gave maximum protection to the plaintiff, and imposed strict liability on the defendant; since then defamation law has been revised in the light of the constitutional guarantee of freedom of expression, and holds that in the case of media defendants, a publication cannot be considered unlawful even if it is incorrect, providing there were reasonable grounds for publication.[41]

South Africa does not have sufficient safeguards for privacy, data protection and online security. The right to privacy is protected in the Constitution, but there is no law in place to give effect to this right. A

35. Shumani Gereda, "The Electronic Communications and Transactions Act", in *Telecommunications Law in South Africa*, eds. Lisa Thornton, Yasmin Carrim, Patric Mtshaulana and Pippa Reburn (2006), link.wits.ac.za/papers/tele-law.html. Also see Paul Furber, "At the Coalface of Cyber-Crime", *ITWeb*, 1 September 2007, www.brainstormmag.co.za/index.php?option=com_content&view=article&id=481:at-thecoalface-of-cyber-crime

36. Film and Publications Board, www.fpb.gov.za

37. ROICA, Section 30(2)(a)

38. Promotion of Equality and Prevention of Unfair Discrimination Act, No. 4 of 2000, Section 10

39. Pierre de Vos, "Malema Judgment: A Re-think on Hate Speech Needed", *Constitutionally Speaking* (blog), constitutionallyspeaking.co.za/malema-judgment-a-re-thinkon-hate-speech-needed; Stephen Grootes, "Malema, a Freedom of Speech Revolutionary?", *Daily Maverick*, 8 May 2011, dailymaverick.co.za/article/2011-09-08-juliusmalema-a-freedom-of-speech-revolutionary; Victoria Bronstein, "What You Can and Can't Say in South Africa", paper commissioned by the Democratic Alliance, n.d., www.da.org.za/docs/548/Censorship_document.pdf

40. Johan Moorcroft, "Defamation on the Internet", *Advocates of Southern Africa*, 22 March 2011, www.southafricanadvocates.info/index.php/legal-articles/64-defamation-on-the-internet

41. Bronstein, "What you can and can't say in South Africa"

draft Protection of Personal Information Bill is being considered by the government, but has not yet been brought forth for discussion in Parliament. South Africa is also in the process of developing a cybersecurity policy, which has been transferred from the Ministry of Communications to the Ministry of State Security, but has not been released publicly at the time of writing.[42]

Self-regulation of internet content

Self-regulation is also widely practiced for online content. The Internet Service Providers' Association (ISPA) is the industry representative body for ISPs recognised by the Department of Communications in terms of the ECT Act. This means that ISPA members have the right to self-regulate, according to a code of conduct adopted in 2008.[43] In order to qualify for immunity from liability in terms of the ECT Act, ISPs that are members of an industry representative body must include a process for handling take-down notifications of content that violates the code. According to the code, members must respect the constitutional right to freedom of expression, as well as the privacy of their communications.[44] However, internet users can send a take-down notice to ISPA, requesting that material considered unlawful be removed. If the user requesting a take-down knowingly misrepresents the facts then s/he is liable for damages for wrongful take-down.[45]

The Wireless Applications Service Providers' Association (WASPA) is the industry body for mobile based value-added service providers. It too has a code of conduct which provides a framework for adult content, and sets in place procedures to protect children from harmful content.[46] The Digital Media and Marketing Association (DMMA) is the industry body for digital publishers, and also has a code of conduct that sets out the expected standards of professional practice of its members.[47] Newspapers operate a self-regulatory system in the form of the Press Council of South Africa, which incorporates a Press Ombudsman and Press Appeals Panel. There has been some uncertainty about whether the system applies to online newspapers, and in 2011 as part of a review of its own processes, the Council recommended that its code should cover the online publications of its members.[48]

Summary of issues

South Africa has an impressive array of laws, policies and regulatory measures impacting on internet access and content. On paper, the country is clearly committed to universality of communications, including of the internet. However, in reality weak policy arrangements coupled with ineffective government interventions and high costs have set the country back when it comes to ensuring universal access to the internet. Disparities in access are highly gendered. With respect to internet content, while strong constitutional guarantees exist for freedom of expression, the effectiveness of these guarantees has been gradually reduced by an array of laws that have chipped away at internet freedom. Self-regulatory measures for internet content are well-developed.

Civil society and the media have also become increasingly concerned about upcoming threats to freedom of expression posed by new or proposed legislation. Parliament is considering a Protection of State Information Bill that seeks to protect valuable state information and classify information on national security grounds. If passed in its current form, the Bill could have a chilling effect on freedom of expression, forbidding whisteblowing about the activities of security agencies if the publication concerned (including an online publication) relies on classified documents and even if there are strong public interest grounds for revealing the classified information. The ANC ruling party has also proposed the reintroduction of statutory regulation for the press in the form of a Media Appeals Tribunal accountable to Parliament, and has proposed that Parliament conduct an investigation into the desirability of this. Media organisations have expressed fears that such a move could pave the way for state control of newspaper content, including their online versions.[49]

42. "South African Cybersecurity Policy Approved", *MyBroadband*, mybroadband.co.za/news/security/45225-southafrican-cybersecurity-policy-approved.html
43. Internet Service Providers' Association, "About ISPA", ispa.org.za/about-ispa
44. Internet Service Providers' Association, "Code of Conduct", ispa.org.za/code-of-conduct
45. Internet Service Providers' Association, "How to request a take-down notice", ispa.org.za/code-of-conduct/takedown-guide
46. Wireless Application Service Providers' Association, "Code of Conduct", www.waspa.org.za/code/waspa_coc_11.6.pdf
47. Digital Media and Marketing Association, "Code of Conduct", www.dmma.co.za/about-us/code-of-conduct
48. Press Council of South Africa, "Review", 7, www.presscouncil.org.za/media/PDFs/report/A5%20report%20for%20web%20pdf.pdf
49. Jackie Bischoff, "SANEF Launches Campaign to Oppose Media Tribunal", *Journalism.co.za*, n.d., www.journalism.co.za/index.php?option=com_content&Itemid=100009&catid=165&id=3337&view=article

Regulation of internet content in South Africa

This section will explore the regulation of internet content in more detail, and considers whether or not this regulation impinges unduly on online freedom of expression and privacy.

The Film and Publications Act

The 1996 Film and Publications Act has been amended several times, and each amendment has broadened the scope for classification and prohibition of material, the type of material covered by the Act, and reduced the independence of the Board and the transparency of its appointment process.

In the 1996 Act, a publication was defined as printed or duplicated matter, pictures and sculptures, recordings for reproduction (with the exception of a film soundtrack), and computer software.[50] This meant that internet content was covered only once it was downloaded or printed out. However, in 1999, the Act was amended to broaden the definition of publication to include "... any message or communication, including a visual presentation, placed on any distributed network including, but not confined to, the internet"[51] – an amendment which effectively gave the Board jurisdiction over internet content. The 1999 amendment also introduced a definition of child pornography that was widened by a 2004 amendment to include descriptions of child sexual abuse, in addition to depictions.[52] The definition of "distribute" was also broadened to include failure to take reasonable steps to prevent access by a person under 18 to classified publications.[53] The 2004 amendment also required ISPs to register with the Board, take all reasonable steps to prevent their services from being used for the hosting or distribution of child pornography, and report the distribution of child pornography.[54]

With respect to the Act's objectives, the 1996 Act regulated the distribution of certain publications, mainly by means of classification, the imposition of age restrictions and the giving of consumer advice, with due regard to the fundamental rights enshrined in the Constitution.[55] However, the 1999 amendment required the Board to regulate the creation and production, possession and distribution of certain publications – to allow for the criminalisation of the creation of child pornography – and replaced the reference to the Constitution with a clause enjoining the Board to have "due regard to the protection of children against sexual exploitation or degradation in publications, films and on the internet". The Act also made the exploitative use of children in pornography, including on the internet, punishable.[56] According to an ISPA advisory, this definition "...is wide enough to be construed as targeting pornography that may in other circumstances be acceptable. For example, portraying someone to look as being under 18 years of age may impact on a large amount of acceptable pornography".[57]

In the 1996 Act, films were subject to pre-classification, but publications were classified only if complaints were received about them and they were found to fall into a classifiable category. However, a 2009 amendment allows anyone to request classification of a publication and further places the onus on the publisher (except newspaper publishers) to submit for classification material that contains sexual violence which violates or shows disrespect for the right to human dignity of any person; degrades a person or constitutes incitement to cause harm; advocates propaganda for war; incites violence; or advocates hatred based on any identifiable group characteristic and that constitutes incitement to cause harm.[58] The Board then submits such material to a classification committee.

In terms of the 2009 amendments, a publication constitutes a "refused publication" if it contains child pornography, propaganda for war or incitement to imminent violence, and the advocacy of hatred based on any identifiable group characteristic and that constitutes incitement to cause harm, unless the publication is a bona fide documentary or has scientific, literary or artistic merit or is on a matter of public interest. "Refused publication" is not defined in the Act, but presumably refers to publications that are banned for possession and distribution. If the publication contains any of the offending material mentioned above, it will be classified XX (prohibited for distribution), unless it has artistic, scientific or public interest merit, in which case it will be classified as X18 and classified to protect children from "harmful

50. Film and Publications Act, No. 65 of 1996, Section 1
51. Tracy Cohen, "Internet Service Providers Association Advisory 3: the Film and Publications Act, No. 65 of 1996 and the Film and Publications Amendment Act, No. 34 of 1999", 22 May 2000, old.ispa.org.za/regcom/advisories/advisory3.shtml
52. Film and Publications Amendment Act, No. 18 of 2004, Section 1
53. Ibid
54. Ibid, Section 12
55. Film and Publications Act, No. 65 of 1996, Section 2
56. Film and Publications Amendment Act No. 34 of 1999, Section 2
57. Cohen, "Internet Service Providers Association Advisory 3", 5
58. Film and Publications Amendment Act, No. 3 of 2009, Section 19 (substitution of Section 16 of the Film and Publications Act)

or age-inappropriate materials". X18 publications can only be distributed by licensed owners of adult premises. The 1996 Act, in contrast, allowed publications to escape classification requirements entirely if they had artistic or scientific merit (with the exception of child pornography).

These 2009 amendments continue to be controversial, and are the subject of Constitutional litigation by SANEF and Print Media South Africa (PMSA). The Constitutional Court heard the case in March 2012, and judgment is pending.[59] These organisations seek to strike down the provision that allows for pre-publication classification on the issues mentioned in the earlier paragraph as unconstitutional. In 2011, the North Gauteng High Court declared this provision unconstitutional, but the government has since appealed this ruling.

A public interest litigation organisation, Section 16, which was granted "Friend of the Court" status, focussed specifically on the implications of the amendments for internet freedom, and argued in its written submission to the Court that the classification specifications were vague and capable of abuse. They were also discriminatory, as newspapers and broadcasters were exempt from this requirement. The self-regulatory system that operates in relation to newspapers, and that is recognised by the Act as a ground for exemption, is less restrictive of freedom of expression than the Act as it accepts post-publication sanction as an appropriate form of sanction for errant publication rather than pre-publication censorship.[60] If a publisher made a mistake and did not submit material that fell into the offending categories before publication, s/he would still be liable for criminal prosecution, which placed small publishers like bloggers and other publishers of user-generated content at particular risk as they were less likely to have access to legal counsel to evaluate their publications than larger, mainstream publishers.

Furthermore, the classification of public interest material in the XX category as X18 was incapable of being enforced for internet content, as this classification category required material to be purchased from an adult shop, which presupposed classification of a physical publication: this meant that material was effectively prohibited, even if it fell within the exemptions. The Section 16 submission described the amendments as "redolent of moral censorship", arguing that "...[it] interposes, between the reader and the creator of the content, the opinion of a state-body that imposes its interpretation upon the exchange of thoughts and ideas. Thus, even before picking up the relevant publication, the would-be adult reader is told by the state that what he [sic] is about to read is harmful or degrading. His ability to form his own opinion, autonomously and independently, and absent a prior moral label from the state, constitutes a pernicious form of thought control".[61]

With respect to the Board's independence, according to the 1996 Act, the Board was appointed by the President of South Africa, on advice of an advisory panel set up by the President to advise him/her on suitable members. The advisory panel was obliged to invite public nominations, and ensure transparency in the appointment process. Nominees could not have a direct or indirect financial interest in the film or publication industry, or hold "an office of profit" in the service of the state.[62] The 1999 amendment changed these arrangements, to ensure that the minister of Home Affairs appoints Board members.[63] The minister was no longer obliged to invite nominations for the Board, but may do so. The amendments also broadened the grounds for removal of Board members and gave the minister powers of removal.[64] This amendment also made it clear that the minister could lodge complaints against publications.[65] While the Board (whose governance structure was renamed the Film and Publications Council) can issue directives of general application, such as classification guidelines, it can do so only in consultation with the minister, which further undermines its independence.[66]

Regulation of Interception of Communications Act

As mentioned earlier the Act that regulates the interception of communications, ROICA, continues to remain controversial on the grounds that it infringes unduly on the right to privacy and freedom of expression. In 2001, the international non-governmental organisation Privacy International warned during Parliamentary hearings on the Bill that it lacked basic safeguards. In finalising the law, Parliament responded to criticisms by introducing

59. Print Media South Africa and another v. Minister of Home Affairs and another CCT 113/11

60. Section 16's written submissions, PMSA and SANEF v Minister of Home Affairs and Film and Publications Board, 5 March 2012

61. Ibid, 10

62. Film and Publications Act, No. 1811 of 1996, Section 7(1)

63. Film and Publications Amendment Act, No. 34 of 1999, Section 3

64. Film and Publications Amendment Act, No. 3 of 2009, Section 6(3); Cohen, "Internet Service Providers Association Advisory 3"

65. Film and Publications Amendment Act, No. 34 of 1999, Section 5-7

66. Film and Publications Amendment Act, No. 3 of 2009, Section 4(a)(1)

judicial, legislative and executive oversight measures to prevent abuses. As a result, the Act ensures that interception centres that carry out the directions report to the Minister of State Security and Parliament's Joint Standing Committee on Intelligence. The designated judge also provides the Committee with an annual report, which becomes publicly available when the Committee's report is released. Furthermore, intelligence activities are certified as being legally compliant by the Inspector General, who is selected by, and reports directly to, Parliament. The Act also disallows communications to be intercepted without a direction being granted by the judge on the grounds specified in the Act, and it requires the judge to be satisfied that less intrusive methods of police or intelligence investigation are not likely to yield the required information.

But Privacy International persisted with their warnings, noting that the US federal wiretapping law contains what they maintained is a higher standard for issuing of interception orders than South Africa's, namely that the application must demonstrate "probable cause" to believe that an individual is committing, has committed, or is about to commit a serious crime. In the South African system, the judge merely has to be satisfied that there are reasonable grounds that a crime has been, or is likely to be committed. Furthermore, directions may also be issued in relation to serious offences that may be committed in future, which may not be constitutional as it allows law enforcement officers to speculate on future acts that have not yet occurred.[67] As a result of their reservations, in a 2006 report on the leading surveillance societies in the world, Privacy International listed South Africa as being among the countries that showed a systemic failure to uphold safeguards.[68]

A key flaw in South Africa's law is lack of public oversight, as the public is provided with too little information to be able to monitor whether the Act is achieving its intended results, namely to fight crime and to ward off genuine threats to national security.[69] While the designated judge's reports are made available as part of the Joint Standing Committee's reports to the National Assembly, they contain little information, and the legislation governing the oversight of the intelligence services, the Intelligence Services Oversight Act, is ambiguous about the content of these reports. As a result, between 2006 and 2008, the designated judge's report merely contained bald statistics on the number of interception orders granted. The designated judge for 2009-2010 issued a more detailed report for that period, but it still falls far short of the reporting obligations needed for effective public oversight. In contrast, in the US federal system, the publicly available annual reports on "wiretaps" in relation to criminal matters include information on the number of interception orders, the major offenses for which orders were granted, a summary of different types of interception orders, the average costs per order, the types of surveillance used, and information about the number of arrests and convictions resulting from intercepts. Furthermore, in South Africa there is no provision for people whose communications have been intercepted to be informed once the investigation is completed, or if the judge turns down the application for an interception direction.[70]

Another source of controversy in relation to ROICA is that the time period for retention of data by telecommunications companies and ISPs is far longer than in comparable jurisdictions, and other jurisdictions merely require targeted data preservation rather than wholesale data retention as required by ROICA. These requirements add considerably to the cost of implementing ROICA, and given that most of the costs of implementation are borne by the service providers, the requirement may prove to be too onerous for small companies, especially ISPs. While provision has been made in ROICA for an Internet Service Providers' Assistance Fund, the fund covers a limited array of the total costs of implementing the Act.[71]

Interception statistics in terms of ROICA have been available since 2008. According to the reports of the various designated judges to the Joint Standing Committee on Intelligence, there have been 826 interception directions granted between 2006 and 2010. Between 2008-2009 and 2009-2010, there was a 120% increase in interception orders (from 189 directions to 416 directions); no information is available to explain this large increase.[72] While there

67. Nazreen Bawa, "The Regulation of Interception of Communications and Provision of Communications Related Information Act" in *Telecommunications Law in South Africa*, eds. Lisa Thornton, Yasmin Carrim, Patric Mtshaulana and Pippa Reburn (2006), 320, link.wits.ac.za/papers/tele-law.html

68. Privacy international, "World's Top Surveillance Societies" www.wired.com/threatlevel/2007/12/worlds-top-surv

69. Jane Duncan, "Another View: Time to Oversee the Officials Who Spy on Us", *Sunday Times*, 30 October 2011, www.timeslive.co.za/opinion/commentary/2011/10/30/another-view-time-to-oversee-the-officials-who-spy-on-us

70. Bawa, "The Regulation of Interception of Communications"

71. Ibid, 330

72. Reports of the designated judges in terms of ROICA, 2006-2010, contained in reports to the National Assembly by the Joint Standing Committee on Intelligence.

is no information about the reasons for interception directions in 2008-2009, in 2009-2010 directions were granted to assist the investigation of drug dealing and drug trafficking, vehicle theft and car hijacks, armed robberies, corruption and fraud, and assassinations, murder and terrorism.[73] Most directions are granted to the Crime Intelligence Division of the South African Police Service, followed by the National Intelligence Agency (NIA, now known as the State Security Agency). By 2009-2010, the designated judge was receiving an average of 35 applications for interception directions a month, and he approved the applications in 94% of cases in the case of the police and 87.3% of cases in the case of the NIA.[74]

The system has proved itself capable of subversion. The *Sunday Times* newspaper has reported that in 2010 intelligence officers duped the designated judge into signing an order to tap the phones of the then Police Commissioner General Bheki Cele, as well as two of the paper's journalists who were reporting on a controversial lease deal the General was implicated in. According to court papers, the intelligence officers lied about who the cellphone numbers contained in the application belonged to. This incident has fuelled fears that other applications to tap the communications of journalists and public figures may have been granted under false pretences.[75]

Significantly, ROICA does not cover foreign signals intelligence, or intelligence derived from any communication that emanates from outside South Africa, or passes through or ends in the country. The state agency that intercepts these signals is the National Communications Centre (NCC), which falls under the Ministry of State Security, and not the OIC. This means that these signals can be intercepted without a warrant; a major lacuna in the law that has been criticised for creating space for violations of the right to privacy on national security grounds. According to the *Mail and Guardian* newspaper, "...this means that you can be bugged completely outside of the law, and without a judge's direction, if your communication involves a party in another country".[76] As a great deal of internet traffic originates outside the country, the interception of this information can take place without judicial oversight, which is wide open to abuse.

In 2008 a Ministerial Review Commission appointed by the then Minister of Intelligence found the unregulated interception of foreign signals intelligence to be unconstitutional, and recommended that the activities of the NCC should be covered by ROICA.[77] This argument was reiterated by several civil society organisations and academics in public hearings on the General Intelligence Laws Amendment Bill in March 2012, which was introduced to amalgamate the various intelligence services into the State Security Agency (SSA). At the time of writing, this Bill is still being considered, but in response to a submissions on this point by the Right2Know Campaign, the Chair of the ad-hoc Committee on the Bill, Cecil Burgess, argued that the international nature of criminal syndicates required law enforcement officials to be proactive and the ROICA warrant procedure took some time, therefore there were circumstances where the intelligence services would need to intercept signals before a warrant could be obtained.[78] This point implied that the Committee may well be open to leaving foreign signals intelligence unregulated.

Take-down notices and acceptable use policies

Self-regulatory mechanisms are less susceptible to state capture, which is why they are preferred for regulation of internet content. However, while self-regulation has many advantages, it is also susceptible to industry capture and as a result can adopt an overly cautious approach towards controversial speech.[79] ISPA's take-down notification procedure does not make any provision for representations to be made by the alleged infringer before the take-down takes place, and there is no in-built right of appeal, which makes the procedure vulnerable to accusations of procedural unfairness and which has led intellectual property lawyer Reinhardt Buys to argue that the take-down pro-

73. J A M Khumalo, "Statistical Briefing by Designated Judge for the Period 1 April 2009 to 31 March 2010", report to the National Assembly of the Joint Standing Committee on Intelligence.
74. Ibid
75. Rob Rose, Stephan Hofstatter and Mzilikazi Wa Afrika, "Bugging: How Cops Lied", *Sunday Times*, 19 May 2012, www.timeslive.co.za/sundaytimes/2012/05/19/bugging-how-cops-lied
76. Heidi Swart, "Secret State: How the Government Spies on You", *Mail and Guardian*, 14 October 2011, mg.co.za/article/2011-10-14-secret-state
77. Ministerial Review Commission in Intelligence, "Intelligence in a Constitutional Democracy", final report to the Minister for Intelligence Services, the Honourable Mr. Ronnie Kasrils MP, 2008.
78. Parliamentary Monitoring Group, "General Intelligence Laws Amendment Bill: Public Hearings", 27 March 2012, www.pmg.org.za/report/20120328-generalintelligence-laws-amendment-bill-b25-2011-public-hearings
79. Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27* (Geneva: United Nations General Assembly, Human Rights Council, 2011), 12, www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

cedures are unconstitutional.[80] These lacunae are significant in view of the propensity recognised in other jurisdictions for take-down notices to be based on contestable grounds.[81] Furthermore, in terms of the ECT Act, a service provider is not liable for wrongful take-down, which acts as a disincentive to scrutinise requests for take-downs carefully; rather liability rests with the lodger of the notice. However, if ISP's do not implement take-down notices they could be liable for hosting illegal content, which incentivises them to err on the side of caution and "take down first and ask questions later", irrespective of the legitimacy of the complaint.[82] The problems with these arrangements were highlighted in 2008, when the Recording Industry of South Africa's (RISA) Anti-Piracy Unit issued take-down notices to ISPA, which then issued the hosting ISP with a take-down notice, and Buys challenged the constitutionality of the take-down procedure.

Another area of self-regulation that requires further examination is the acceptable use policies of South African ISPs and the extent to which they pass constitutional muster. An overview of the policies of some of the largest ISPs in South Africa suggests a tendency to identify prohibited content that would otherwise be protected speech under South Africa's constitution.

For instance, MWEB's acceptable use policy states that it prohibits use of the IP services in a way that is "...harmful, obscene, discriminatory... constitutes abuse, a security risk or a violation of privacy...indecent, hateful, malicious, racist... treasonous, excessively violent or promoting the use of violence or otherwise harmful to others".[83] Most of the quoted grounds are vague and would cover speech that would ordinarily receive constitutional protection, which implies that MWEB has adopted an inappropriately censorious approach towards controversial speech. iBurst's policy is even more restrictive in that it forbids publication of illegal material which it defines as including material that is obscene and discriminatory. However, it also forbids material that "...could be deemed objectionable, offensive, indecent, pornographic, harassing, threatening, embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful". There can be little doubt that this provision is unconstitutional, given its over-breadth, which covers offensive and not just harmful material, whereas the constitution requires a harms test to be applied before the right can be limited on justifiable grounds.[84] In contrast, Internet Solutions' policy restricts prohibited content to "...copying or dealing in intellectual property without authorisation, child pornography and/or any unlawful hate-speech materials".[85] The Codes of Conduct of WASPA and the DMMA are also unduly restrictive of freedom of expression and use highly subjective measurements of unacceptable material, covering material, for instance, that merely causes grave and widespread offence.

Awareness

This section assesses whether there is widespread awareness about the issues in the previous section, and whether civil society is organising to address problems and threats to internet rights. It maps the civil society landscape, identifying the key organisations of human rights defenders, and assesses their effectiveness in addressing internet rights.

South Africa does not have an organisation dedicated to internet rights. However, the country has a lively civil society sector that acts as an important check against unrestrained use of state and private power. An important positive development has been the recent formations of civil society coalitions around specific issues. The two most prominent coalitions are:

- SoS: Support Public Broadcasting Coalition is a civil society coalition which was formed in 2008 and which focuses on addressing the multiple crises at South Africa's public broadcaster, the South African Broadcasting Corporation (SABC). It also lobbies for citizen-friendly policies, laws and practices for public and community broadcasting, and advocates for an effective and independent communications regulator.[86] The coalition has made South Africa's digital

80. Rudolph Muller, "Local Websites in Danger", *MyBroadband.com*, mybroadband.co.za/news/internet/5948-local-websites-indanger.html
81. Jennifer Urban and Laura Quilter, "Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millenium Copyright Act", *Santa Clara Computer & High Technology Law Journal 22*, 4 (2006): 621, lquilter.net/pubs/UrbanQuilter-2006-DMCA512.pdf; Tyler Moore and Richard Clayton, "The impact of Incentives on Notice and Take-down", Seventh Workshop on the Economics of Information Security (WEIS 2008), 25-28 June 2008, www.springerlink.com/content/g856v7w02303n620
82. Muller, "Local Websites in Danger"
83. MWEB, "MWEB Acceptable Use Policy", www.mweb.co.za/legalpolicies/GeneralPage/AcceptableUsePolicy.aspx
84. IBurst, "Acceptable Use Policy", www.iburst.co.za/documents%5Clegal%5Cdocument_2.pdf
85. Internet Solutions, "Acceptable Use Policy", www.is.co.za/legal/Pages/default.aspx
86. SoS, "About SoS", www.supportpublicbroadcasting.co.za/about

migration process part of its core work, and is one of the few civil society organisations actively involved in the lobbying around the process.[87] SoS has also made a submission on the draft Local and Digital Content Development Strategy.

- Another civil society coalition, the Right2Know Campaign, was established in 2010 to campaign for a Protection of State Information Bill that meets what it refers to as its "seven point freedom test". The campaign has been successful in raising public consciousness about the Bill and mobilising opposition. It has also managed to ensure significant legislative amendments to the Bill. More recently, R2K has also begun to conduct advocacy on broader issues relating to the transparency and accountability of the security cluster. In the context of this advocacy, R2K has argued for greater oversight of monitoring and interception of communications, especially foreign intelligence signals.[88] R2K does not have any dedicated activities, however, on internet rights.

- Other South African-based organisations taking up issues that touch on internet rights are as follows (not an exhaustive list):

- Media Monitoring Africa, which promotes quality media in Africa from a rights-based perspective through acting as a watchdog of media ethics and freedom. It undertakes advocacy on these issues as well, and includes online media rights in its work.[89]

- The Freedom of Expression Institute (FXI), which was formed in 1994 and whose mandate is to fight for and defend freedom of expression, oppose censorship and to fight for access to information and media diversity. The FXI has on occasion taken up cases of online censorship.

- Section 16, which advocates for law reform in relation to freedom of expression and access to information, including online.[90]

- Genderlinks focuses on promoting gender equality, especially through the media, in the SADC region and comments on and publicises issues around gender equality and media and ICTs.[91]

- The South African National Editors' Forum (SANEF) is an association of editors and journalism educators. It engages in advocacy on media freedom issues, which may also extend to online media.[92]

- While less public than SANEF, ISPA and WASPA also undertake advocacy on behalf of their members on issues affecting internet freedom, and were active in making representations to amendments to the Film and Publications Act that they felt threatened the rights of their members.

- The Open Democracy Advice Centre (ODAC), which conducts litigation and advocacy around the Promotion of Access to Information Act and the Protected Disclosures Act. ODAC has also been instrumental in organising civil society participation in the Open Governance Partnership, and in that context has raised the need for the South African government to embrace open data principles.[93]

- The Alternative Information Development Centre (AIDC), which was formed in 1996 to promote social justice in South Africa's then newly-established democracy. It ensures the dissemination of progressive alternative perspectives through participatory peoples' media including social media, and has also undertaken advocacy on issues affecting internet rights.[94]

- The South African NGO Network (SANGONeT), provides non-governmental organisations with a range of tools and services, but is not really involved in advocacy on South African internet rights. SANGONeT publishes an online newsletter focussing on the NGO sector called NGO Pulse.[95]

- The Link Centre is based at the University of the Witwatersrand, conducts research and training on ICT-related issues, and offers post-graduate courses. It also undertakes advocacy in the form of submissions to various fora.[96]

87. SoS – Support Public Broadcasting, "Policy Submission on the Digital Dividend", 23 March 2011, www.supportpublicbroadcasting.co.za/library/entry/sos_-_policy_suggestions_on_the_digital_dividend
88. Right2Know Campaign, "Submission to the Ad-hoc Committee of the National Assembly on the General Intelligence Laws Amendment Bill", 16 March 2012, d2zmx6mlqh7g3a.cloudfront.net/cdn/farfuture/mtime:1333357073/files/docs/120322right2know_1.pdf
89. Media Monitoring Africa, "About Media Monitoring Africa", www.mediamonitoringafrica.org/index.php/about
90. Section 16, "About us", www.sectionsixteen.org/newsletters/index.cfmy=category_home&company=1&subsection=9&newsletter=o
91. Genderlinks, "About us", www.genderlinks.org.za/page/about-us
92. SANEF, "About Sanef", www.sanef.org.za/about
93. South African Open Governance Activity, opengovpartners.org/za
94. AIDC, "About AIDC", www.aidc.org.za/index.php?option=com_content&view=article&id=47&Itemid=76
95. SANGONeT, "About SANGONeT", www.ngopulse.org/about
96. Link Centre, link.wits.ac.za

- The South African Chapter of the Creative Commons popularises the use of creative commons licences that seeks to protect the copyright in a way that acknowledges the need for access to information in the digital era.[97]
- Research ICT Africa conducts research, training and capacity building on ICT-related issues in 20 African countries, including South Africa, and undertakes advocacy on the ICT policy environment in South Africa.[98]

There are several online sites devoted to digital media issues, and other that touch on digital media-related issues, such as MyBroadband.com, ITWeb, The Media Magazine, FreeAfricanMedia, Hellkom and Daily Maverick. These online sites are important repositories of information and analysis on issues affecting the internet, and keep their readers informed and engaged in issues that affect their rights. Largely, these sites have not become engaged in direct advocacy in support of internet rights, but have the potential to do so.

This brief overview shows that civil society and the media space is rich with activity on internet-related issues. However, the fact that serious incursions have been made into internet freedom suggests that civil society advocacy on internet rights has not been sufficiently robust, and that the advocacy that has taken place has been piecemeal, relatively uncoordinated and of limited impact on key issues. In spite of the proliferation of IT-related sites, reflecting the complexity and breadth of the ICT sector, there has been little public education work on the impact of these creeping erosions of internet freedom. This is in contrast to legacy media freedom issues, where threats to this freedom have been met with strong reactions from civil society, and hence concessions by the government and Parliament. No ongoing monitoring is taking place of decisions being made by the Film and Publications Board or the Equality Courts or ISPs, for instance, to assess their impact on online freedom. As a result, it is impossible to assess the true import of the problems outlined in the earlier section. It has been shown that coalitions work well in South Africa when it comes to advocacy in rights-related issues, especially if they have a mass base, and what should be considered is the possibility of a coalition-based approach to advocacy on internet rights in South Africa.

97. Creative Commons South Africa, www.creativecommonsza.org
98. Research ICT Africa, "About Research ICT Africa", www.researchictafrica.net/about.php

Impact on other rights

This section focuses on the rights that are affected by the problems identified in the earlier section. With respect to the universality of the internet, the widespread penetration of mobile phones has expanded access to the internet. But because of the inherent technical limitations of mobile phones, they cannot be used as easily as fixed-line connections via ADSL for accessing large amounts of information. This problem could fail to narrow and in fact even sharpen the divide between the information-haves and information have-nots. The cost of connectivity is possibly the single largest barrier to popular access to and usage of the internet, which impacts negatively on both freedom of expression and access to information as poor users, women and youth are affected disproportionately, making them even more vulnerable to economic and social marginalisation and therefore impacting negatively on their right to equality. Linguistic diversity is sadly lacking on South African-orientated sites, which impacts negatively on the right to cultural and linguistic identity of those who do not consider English their home language or mother tongue. To this extent, language acts as a significant barrier to online usage for many South Africans. While there are plans to ensure the roll-out of a national broadband infrastructure, and to ensure a greater diversity of online content, the targets set for the roll-out are not ambitious, and may fail to ensure that access to the kind of high-speed broadband needed to ensure social and political participation becomes a reality.

The lack of affordable internet access limits the potential of the internet to be put to a range of beneficial uses, such as improving service delivery and encouraging political participation, and therefore impacts on a range of rights. One of the most significant impacts is on the right to education. While the government made proposals as far back as 2001 for a special e-rate to apply to schools to facilitate access to the internet, and ICASA held public hearings on the matter in 2010, the rate has still not been implemented.[99] These problems make it difficult to ensure widespread connectivity to the internet in schools, which in turn reduces the ability of learners to develop the skills needed to participate meaningfully in the information society. Teachers and learners in unconnected schools are also deprived of rich online educational resources.[100]

99. Rudolph Muller, "E-rate Battle Stage Set", *Mybroadband*, 18 February 2010, mybroadband.co.za/news/telecoms/11537-e-rate-battle-stage-set.html
100. J Nonyane and N Mlitwa, "ICT Access and Use in Rural Schools in South Africa: A Case Study in Mpumalanga Province", unpublished paper, Cape Peninsula University of Technology

Lack of affordable access also impacts negatively on e-health deployment. The Presidential National Commission on the Information Society and Development viewed ICTs as vehicles to bridge the gap between rural and urban healthcare by linking medical practitioners who are separated geographically. However, lack of access to an internet connection has been cited as one of the most significant barriers to the realisation of the potential of e-health in rural clinics.[101] Political participation is also adversely affected as it makes it difficult for citizens to participate in political activities and to interact with government online, including accessing government services.

Unduly restrictive internet content regulation also impacts negatively on a range of rights. In the past ten years, South Africa lawmakers have demonstrated a tendency to prioritise national security over civil liberties, resulting in insufficient privacy safeguards, and the fact that South Africa still lacks privacy legislation exacerbates the problem. The overly broad powers of the cyber-inspectors provided for in the ECA Act potentially threatens the right to privacy. Furthermore, the lack of basic safeguards to protect the right to privacy when communications are intercepted in terms of ROICA also creates space for abuses of this right, and indeed evidence has emerged of abuse. However, as with the application of the ECA Act, too little information is available to establish whether abuses are occurring on a widespread basis. The inability of civil society to hold the government to account in this regard is in itself a concern that needs to be addressed.

The lack of safeguards may well lead to users self-censoring out of fear of their communications being intercepted. In the run up to the ANC's previous elective conference in 2007, evidence emerged of the communications of some of the then President Thabo Mbeki's political opponents being intercepted, which led to the Ministerial Review Commission mentioned in the earlier section. Ahead of the next elective conference in Manguang, politicians and trade unionists have also expressed fear that a similar problem is occurring, leading to extreme caution in communicating any information and expressing opinions about the suitability of the incumbent Jacob Zuma for office and a possible successor.[102] Such fears are likely to have a chilling effect on the right to engage in free political activity.

With respect to freedom of expression, the fact that internet content was brought under the jurisdiction of a government agency with limited independence, the Film and Publications Board, with hardly any public debate about its implications, is deeply concerning. Both the Film and Publications Act and the Equality Act have stretched definitions of hate speech beyond what is constitutionally permissible. In the process, the robust exchange of opinions on a range of issues could be discouraged on the basis that they constitute hate speech, especially if these opinions cause widespread shock or offence.

The self-regulatory system for internet content is also not without its flaws. In order to escape liability when they are informed, as argued it is very possible that ISPs are adopting an overly cautious approach to complaints they receive on allegedly illegal material. Furthermore, the fact that major ISPs have largely adopted acceptable use policies that restrict legitimate speech, and not just speech that does not receive Constitutional protection, is of concern. The fact that ISPA's take-down procedure does not allow the alleged infringer the right to make representations or to appeal a decision is an additional factor that risks tilting the self-regulatory regime towards censorship.

Conclusions and recommendations

South Africa largely respects online freedoms, and to this extent the country could be considered to have a free online media environment. Many of the instances of internet censorship apparent in more repressive countries, and outlined by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, are absent in South Africa.[103] Bloggers, for instance, are not criminalised for expressing their views, as they are in much more repressive contexts. The fact that ISPs are not held liable for internet content – unless they are informed of the existence of illegal content and they fail to take the content down – is a positive feature of the ECT Act. There is no evidence of internet users being disconnected, even if they violate intellectual property laws. Cyber-attacks have become a growing problem in South Africa, but

101. Nkqubela Ruxwana, Marlien Herselman and Pieter Conradie, "ICT Applications as E-health Solutions in Rural Healthcare in the Eastern Cape Province of South Africa", *Health Information Management Journal*, 39, 1 (2010): 17-26

102. Njanji Chauke, "Mduli Admits Writing a Letter to Zuma", *SABC News.com*, 11 May 2012, www.sabc.co.za/news/a/414815804b35447fa7d4efe756e8533f/Mduli-writes-to-Zuma

103. La Rue, *Report of the Special Rapporteur*

these are largely perpetrated by criminals against businesses;[104] there is no evidence of such attacks being used against political opponents.

However, there are indications that the conditions for internet rights are not optimum and need to be improved. According to La Rue's report, there are legitimate grounds for restricting certain types of information such as child pornography, hate speech, defamation, and direct and public incitement to commit genocide. However, any limitation must meet a three-part cumulative test, which ensures that limitations are predictable and transparent: they must be legitimate and they must be necessary and proportional to the aim. He noted that many countries are placing undue restrictions on the internet.[105] Three aspects of this trend cited in his report are relevant for South Africa: criminalisation of legitimate expression, arbitrary blocking and filtering of content, and inadequate protection of the right to privacy and data protection. With respect to the first, it is apparent from an analysis of the various amendments to the Film and Publications Act that the scope for criminalisation of "unacceptable" content has been gradually expanded beyond the constitutionally recognised limitations on freedom of expression. With respect to the second, aspects of the self-regulatory system for internet content are also unduly restrictive of freedom of expression. With respect to the third, safeguards to protect abuses of the government's monitoring and interception of communications capability are inadequate.

La Rue has also argued for government to prioritise internet access, given that it has become an indispensible tool for realising human rights, which includes making the internet available, accessible and affordable.[106] Where access is present, La Rue has also called on governments to ensure that usable, meaningful content is provided online. South Africa clearly has some way to go in realising these three dimensions of universality. A key weakness in South Africa's ICT landscape has been a confused policy framework that attempts to balance conflicting objectives, but that has on balance allowed excessive profit-taking by parastatal and private network operators at the expense of universal service. In the case of Telkom, the Department of Communications, which is also the custodian of Telkom's shares, has protected the parastatal from competition to enable it to meet universal service targets. However, it has largely failed to meet these targets because the company sought to extend the network on commercial principles, which led to massive churn as users could not afford the rising costs of the service. Cellphone network operators have been largely unregulated by policy, which has allowed them to entrench their dominance relatively unchallenged.

An added dimension to the problem is that ICASA has been weakened by the Department of Communications through a variety of measures, including underfunding, and an erosion of its administrative and institutional independence. The regulator's weakness has meant that it cannot hold the network operators to account sufficiently, which has exacerbated the problems mentioned above. These weaknesses also point to the ineffectiveness of USAASA in promoting universal service and access to ICTs. Like ICASA, USAASA has struggled to assert itself independently of the Department of Communications, and has been plagued by ineffective management.[107]

The ANC has attempted to address weaknesses in the ICT landscape, including the affordability problem, by developing a draft ICT policy framework for its forthcoming national conference. It remains to be seen if this development, as well as the Department's ICT Policy Review, will address ongoing problems of affordable access to ICTs generally, including the internet.

The following recommendations are made for civil society:

- A coalition of existing organisations around internet rights could be considered. Rather than forming another coalition, exploratory discussions could be held with the Right2Know Campaign and the SoS: Support Public Broadcasting Coalition to establish an internet rights project, which could then become a campaign focus among their members. These coalitions could also be broadened to include organisations that specialise in IT issues and that therefore should have an interest in internet rights. Not only will this coalition lobby to remove the current restrictions in internet content, but it will organise communications users, especially the poor, and campaign for affordable to access to communications. These organisations should be provided with the necessary assistance to build the capacity of their

104. Charlie Fripp, "Cyber-attacks Remain Problematic", *IT News Africa*, 19 October 2011, www.itnewsafrica.com/2011/10/cyberattacks-remain-problematic

105. La Rue, *Report of the Special Rapporteur*

106. Ibid

107. Lewis, "Achieving Universal Service"

members to advocate on questions of internet freedom.

- Audits should be conducted of decisions of the following institutions, to establish whether online freedom is being unduly compromised: decisions of the Film and Publications Board that impact on online freedom; ISPA take-down notices; interception reports of the designated judge in terms of ROICA; and activities of the cyber-inspectors set up in terms of the ECT Act. Where information is not publicly available on their activities, Promotion of Access to Information Act requests should be filed to obtain the information, and if the information is refused, then the right should be enforced through litigation. The findings of these audits should be released publicly to build public awareness of the extent of internet rights.
- Monitoring of the decisions of these institutions should also take place on an ongoing basis. Where internet rights violations take place, these should be publicised and the responsible institution "named and shamed".
- An audit should be conducted of the acceptable use policies of ISPs, and where necessary these ISPs should be approached to change these policies if they are unduly restrictive of online freedom.
- ISPA should be approached to reconsider its take-down notification procedure to ensure that it is procedurally fair. This recommendation and the one above are designed to address La Rue's concern that "...corporations also have a responsibility to respect human rights, which means that they should act with due diligence to avoid infringing the rights of individuals".[108]

The following recommendations are made for Parliament and government:

- Parliament should amend ROICA to ensure that people whose communications have been intercepted should be informed after the completion of investigations, or if the designated judge refuses to grant an interception direction. ROICA should also be made applicable to foreign signals intelligence.
- The Intelligence Services Oversight Act should also be amended setting out the required content for reports of the designated judge in ROICA. At the very least, annual reports should include the following information: the number of directions granted; the offences for which orders were granted; a summary of types of interception orders; the average costs per order; the types of surveillance used; and information about the resulting arrests and convictions.
- The Film and Publications Bill should be amended to ensure that the Board's jurisdiction does not extend to the internet. Alternatively, if this amendment is not winnable then its jurisdictions should only extend to child pornography, hate speech, propaganda for war and incitement to imminent violence, and that if internet content has artistic, scientific, or public interest merit, then it does not have jurisdiction over such content at all. Furthermore, the independence of the Board should be enhanced, and the Board should be made accountable to Parliament. This will bring the Board into line with La Rue's recommendation that "any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial or other unwarranted influences".[109] The pros and cons of collapsing the Board into ICASA, given the latter's constitutionally protected independence, and given the inevitable convergence of content classification systems, should also be evaluated.
- The Protection of Personal Information Bill should be expedited to ensure legislative protection of the right to privacy.
- The Department of Communications' ICT policy should conduct an honest assessment of the strengths and weaknesses of the communications environment, including an assessment of the profit-taking practices of network operators and its own role in allowing these practices to continue, either through acts of commission or omission. The review should also identify structural conflicts of interest in the communications environment that impede universality, and provide solutions to these problems.

108. La Rue, *Report of the Special Rapporteur*, 21

109. Ibid, 20

- Through the above review, weaknesses in ICASA's administrative, financial and institutional independence must be identified and improved to ensure that it becomes a more effective regulator, less susceptible to governmental and industry capture.
- The review also needs to ensure that ICASA regulates the costs of communications much more effectively to ensure affordable access to communications.
- The Department of Communications' Broadband Policy should be accompanied by an implementation plan and budget and should be amended to increase download speeds and penetration rates for households. The department's ICT review should also actively canvass synergies between broadcasting and broadband to ensure that the benefits of converged networks are optimised and made widely available.
- The mandate of USAASA should be reviewed to ensure that it makes a meaningful difference to universality by providing targeted subsidies that improve access to communications. USAASA must be mandated to develop access plans for women and youth especially to address the yawning digital divide for both social groups. ■