Innovation, Regulation and the Digital Environment: The South African Case

*Mitchell Lüthi**

Abstract

It is self-evident that the law, which is often considered to be slow moving at best, has a tendency to lag behind innovation and changes within the system it governs. Despite what appears to be an intrinsic resistance to change, there is much to be said about the legal certainty, the consequential continuity as well as the stability such a system affords those who find themselves within it. In contrast, technology within the digital environment develops and changes at a rapid pace, almost as fast as it proliferates. The innovativeness and productiveness of such an industry often leaves little time for reflection upon salient applicable legal principles involved. Unfortunately, when steps are finally made to modernise the law and to regulate the proliferation of information in such an environment, one seldom finds that the law is implemented smoothly and without conflict or contradiction. This essay attempts to highlight some of these problems and to address a number of the fundamental issues raised by the new policies, amendments and legislation that presume to deal with the digital environment in South Africa.

I. Introduction

For developing countries, access to knowledge and information plays a fundamental role in the growth of sustainable development. The evolution of information and communication technologies (ICTs) has, seemingly, provided a mechanism by which such resources can be accessed by users in much of the developing world. The internet allows for instantaneous communication, dissemination of data and information and the access to tools and mechanisms which are crucial to the goal of sustainable development and growth. However,

* The author is an LL.M candidate at the University of Cape Town in Cape Town, South Africa.

the speed by which information can be disseminated, files distributed and content shared comes at a cost. The internet provides a potential platform for hate speech, racism, the distribution of child-pornography, gratuitous violence and the large-scale infringement of copyright-protected materials. As such, striking a balance between allowing for the free flow of information, which is so vital to developing nations, and the regulation and policing of the digital environment is imperative. This essay examines, with a focus on South Africa, the policies and law relating to the digital environment and the impact they have on development. This approach will take into account, *inter alia*, the policy choices adopted in the developed and developing world, the consequences of such policies and the applicability of similar methods to South Africa's unique environment. In doing so, this essay will examine the role of ICTs in the advancement of democratic principles and contrast this with the nature of the current and proposed regulatory framework. This will require an examination of the type of content to be regulated, the Film and Publication Board's draft and final version of its Online Regulation Policy, the Film and Publications Amendment Bill, the Cybercrimes and Cybersecurity Bill and the Regulation of Interception of Communications and Communication-related Information Act. Finally, this essay will conclude with some comments on the impact the approach taken by South African policy makers may have on economic and social development.

II. ICTs and the Information Society

Before such an examination can begin, it is pertinent to briefly define ICTs and to place them within their larger social and political framework. This is so as to elucidate what is at issue, and to create the basis for the focus of this examination. ICTs are regarded as a vital tool in the battle against global poverty and economic disparities.[1] In support of this there is a growing amount of anecdotal, economic, and theoretical evidence which identifies the role of information technology in growth and development.[2] In the financial sector, the internet may have a significant impact on the growth and functioning of markets and firms. In addition to this, at the micro level, there has been a high return on investments in computers and mobile technology across a range of industries, when compared to other types of capital. In the presence of skilled labour, it is expected that

1 Kenny C, 'The internet and economic growth in less-developed countries: A case of managing expectations?' 31 *Oxford Development Studies* 1, 2003, 99.

2 Kenny C, 'The internet and economic growth in less-developed countries', 99.

this impact will be felt at a macroeconomic level.[3] As a result, new markets have been created which creation has led to an increase in businesses and jobs. These benefits are not restricted to the financial sector. Indeed, the internet facilitates freedom of expression by making information freely and easily accessible which, in turn, allows for the freedom to disseminate and exchange ideas. The changes produced by ICTs have the ability to influence various aspects of society and are starting to be felt in the education system.[4] The implementation of teaching methods that incorporate ICTs may operate to enhance the quality of education in a number of ways and can promote a shift to a learner-centred environment.[5] Moreover, engaging with ICTs can allow for enhanced teacher training and the development of the basic skills that are becoming more and more valuable in the digital era.[6] The shift to a learner-centred environment, in part, can be enabled by the inclusion of the internet and computers, both in class and in studying activities. The use of these technologies in order to facilitate a new form of teaching could result in a departure from the traditional approach of memorisation and rote learning.[7] A consequence of this may be a focus on individual research, academic freedom and the creation of a more open and accessible learning environment that encourages individual thought and expression.

As a result of the fact that developed nations typically have a greater stock of human capital and higher levels of educational attainment, these benefits will accrue therein with relative ease.[8] However, the adoption and adaptation of such methods in the developing world may provide a means by which the effects of such disparity are mitigated. Furthermore, open access initiatives allow for the dissemination of educational materials, learning tools and development methods.[9] Such initiatives are of great value to the developing world and, in particular, to economies that are not sufficiently developed to invest in the education system and, consequently, human capital. ICTs provide the opportunity for the developing world to take advantage of the research and development of the developed

3 Kenny C, 'The internet and economic growth in less-developed countries', 101.

4 Mikre F, 'The role of information communication technologies in education: Review article with emphasis to the computer and internet' 6 *Ethiopian Journal of Education and Sciences* 2, 2011, 1.

5 Tinio, *ICT in education* United Nations Development Programme, New York, 2003, 7.

6 Tinio, *ICT in education*, 7.

7 Tinio, *ICT in education*, 7.

8 Sykes A, 'TRIPS, pharmaceuticals, developing countries, and the Doha Solution' 3*Chicago Journal of International Law* 1, 2002, 2.

9 Contreras J, 'Open access scientific publishing and the developing world' American University Washington College of Law, Washington College of Law Research Paper Number 39, 2012 — http://digitalcommons.wcl.american.edu/fac_works

world and to incorporate such knowledge into their own respective education systems.

ICTs also provide a platform for human rights and political activism. Such a platform can be used to expose rights violations and to introduce campaigns against the administrations responsible for the violation of these rights.[10] Through the use of websites, emails, video recordings and message boards, many non-governmental organisations galvanise action, by the national and international community, against corrupt officials and rights violators.[11] The internet provides a mechanism by which a variety of international groups can coordinate and exchange information before taking active steps and alerting politicians or the media.[12] An example of this is the 'Arab Spring' of 2011, in which social media played a fundamental role in the downfall of the political establishments of Egypt and Tunisia, and contributed to the mobilisation of the masses in Syria and Bahrain.[13] Moreover, social media can be used as a tool for transparency and openness.[14] This is particularly the case when it comes to countering state-owned media outlets and propaganda. An example of this can be found in Australia during the 2007 political campaigns. The Australian media openly supported the conservatives and selectively reported the results of their own polls.[15] Blogs, websites and online social media networks provided contrasting views to the biased media coverage and provided a means by which Australian citizens could actively engage in the discussions and debate surrounding the political campaign.[16] Aside from political discourse, mobilisation and transparency, ICTs also offer possibilities for improved governance and efficiency, engagement and participation.[17]

---

10 Burnheim S, *The right to communicate: the internet in Africa*, Article 19 Publications, London, 1999, 5.

11 Selian A, 'ICTs in support of human rights, democracy and good governance' International Telecommunication Union, August 2002 – <https://www.itu.int/osg/spu/wsis-themes/humanrights/ICTspercent20andpercent20HR.pdf> on 16 November 2016.

12 Selian A, 'ICTs in support of human rights, democracy and good governance' International Telecommunication Union, August 2002 – <https://www.itu.int/osg/spu/wsis-themes/humanrights/ICTspercent20andpercent20HR.pdf> on 16 November 2016.

13 PONARS Eurasia Policy Memo No. 159, *The role of information communication technologies in the 'Arab Spring'*, 2011, 1.

14 Betrot C, Jaeger P and Grimes J, 'Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies' 27 *Government Information Quarterly* 3, 2010, 267.

15 Betrot C *et al*, 'Using ICTs to create a culture of transparency', 267.

16 Bruns A, Wilson J and Saunders B, 'Citizen journalism as social networking: Reporting the 2007 Australian federal election' in Allan S and Thorsen E (eds) *Citizen Journalism: Global perspectives*,Peter Lang, 2007,197.

17 Guchteneire P and Mlikota K, 'ICTs for good governance – Experiences from Africa, Latin America and the Caribbean' IST-Africa Conference and Exhibition hosted by the Government of Namibia,

In Kenya, the Electronic Graft Management project offers a means by which anonymous users can report corruption in their districts.[18] In Estonia, ICTs have been used for civic consultation and are used to enable citizens to comment on draft laws, effectively including them in the policy-making process.[19] As such, ICTs make for a more accountable administration and a more openly democratic society. While the benefits of the full integration of ICTs in the developing world would be numerous, the application of such technologies and tools, in Africa, has not occurred unhindered.

III. ICTs in Africa

The period of 1996 to 1998 saw the number of African countries with full internet access in capital cities nearly triple. Despite the rapid growth in internet connectivity, its penetration is still largely confined to urban areas within the more developed nations.[20] While internet usage levels are slightly higher than twenty percent and mobile subscriptions are just under seventy percent, the aggregate indicators mask glaring disparities.[21] A vast majority of African countries enjoy internet penetration levels of less than 10 percent, which is considered to be well below the 20 percent threshold required for countries to reap the economic benefits of broadband investments.[22] A major obstacle to its spread in many countries is due to government monopolies in telecommunications and the vested interest they have in obsolete technologies and high cost structures.[23] An example of this is the long spanning dispute between Telkom and various internet service providers in South Africa from 1996. The Internet Service Providers Association (the ISPA) challenged the role of the state-owned company before the Competition Commission and then in the Supreme Court of Appeal.[24] A number of complaints had been lodged against Telkom by the service providers and was referred to the Competition Commission, where it was alleged that Tel-

Windhoek, 7-9 May 2008, 1.

18 Onunga J, 'Kenya – Bursting corruption using the internet' Cddc.vt.edu, 1.

19 Guchteneire P and Mlikota K, 'ICTs for good governance – Experiences from Africa, Latin America and the Caribbean', 2.

20 Molawa S, 'The first and third world in Africa: Knowledge access, challenges and current technological innovations in Africa' First International Conference on African Digital Libraries and Archives, Addis Ababa, 1 July 2009, 1.

21 Internet Society, *Internet development and internet governance in Africa*, 2015, 1.

22 Internet Society, *Internet development and internet governance in Africa*, 2015, 1.

23 Burnheim, *The right to communicate*, 5.

24 *Competition Commission of South Africa v Telkom SA Limited* (2008), Supreme Court of Appeal of South Africa.

kom was abusing its position as sole provider of telecommunication services in order to undercut prices of private internet service providers (ISPs), who had to bear the expense of leasing Telkom's lines for their own clients.[25] This occurred through various pricing mechanisms that Telkom offered to its wholesale ISP buyers. The prices Telkom offered amounted to a margin squeeze and reduced the competitiveness of other ISP providers in the market who, as a result of Telkom's monopoly, had to run their services through Telkom.[26] After being referred back to the Competition Tribunal, the parties reached a settlement which included an admission of guilt; a financial penalty; functional separation between Telkom's retail and wholesale divisions along with a transparent transfer pricing programme that would ensure non-discriminatory service provisions by Telkom to its retail division and ISPs.[27] This prevented the state-owned company from exercising its monopoly over internet services in an abusive manner, thus reducing the potential for anti-competitive practices and preventing the state from having absolute control over South Africa's internet usage.[28]

Research has shown that free and open access to the internet has fostered economic activity, helped facilitate the exchange of ideas and information and operated to better social relations between different ethnic groups.[29] Despite this, internet censorship and the restriction of access is becoming more common.[30] Although the direct censorship of internet content has not, in the past, been as significant a problem in Africa as it has been with the more traditional forms of media, there has been a growing trend towards more subtle forms of censorship, particularly in transitional democracies.[31] This trend has taken a more despotic turn of late as a number of African countries have implemented telecommunication and social media shutdowns. Ghana has been widely lauded by the international community as a role model for democratic practice in West Africa.[32] Despite this the government has threatened, on a number of occasions, to block

25 *Competition Commission of South Africa v Telkom SA Limited* (2008), Supreme Court of Appeal of South Africa, 6.

26 *Competition Commission v Telkom SA SOC LTD* (2013), Competition Tribunal of South Africa, 3.

27 *Competition Commission v Telkom SA SOC LTD* (2013), Competition Tribunal of South Africa, 6.

28 Burnheim, *The right to communicate*, 3.

29 Eluwole O, Udoh N and Ojo O, 'The impact of internet on African education and culture' 4 *International Journal of Business, Humanities and Technology* 3, 2014, 73.

30 Li J, 'Internet control or internet censorship? Comparing the control models of China, Singapore and the United States to guide Taiwan's choice' 14 *Journal of Technology, Law and Policy* 1, 2013, 38.

31 Burnheim, *The right to communicate*, 1.

32 Armah-Attoh D, Robertson A, 'The practice of democracy in Ghana: Beyond the formal framework' Afrobarometer, Briefing Paper Number 137, 2014, 1 —http://afrobarometer.org/publications on 18 November 2016.

social media access on the eve of, and on Election Day.[33] Citizens in Congo, Uganda, Chad and Ethiopia have discovered, to the detriment of the right to free speech, that elections have become a particularly popular time to crack down on social media platforms.[34] In Zimbabwe, following growing civic unrest and protests, the government blocked access to a number of popular social media platforms and websites.[35] This occurred less than a week after the United Nations Human Rights Council declared that online rights must be protected and, notably, condemned any disruptions to internet access.[36] Although these actions may be unlawful and constitute ad hoc responses to political unrest and dissension, there is a growing trend among developing nations to legislate limitations and restrictions that curb internet and constitutional freedoms. While, *prima facie*, they do not appear to be as shocking or reactionary, they may have long term effects which are just as damaging.

IV. User-Generated Content in Brief

While there are a number of laws pertaining to the use of ICTs, the focus, in part, seems to have turned to content that is created, uploaded and disseminated by individual users otherwise known as user-generated content. As such, it is pertinent to briefly define User-Generated Content (UGC) and the role it plays in the digital environment. UGC is a term that has been used to describe a broad range of internet-based activity, from blogging and streaming, to file-sharing.[37] Gervais offers a functional approach and characterises it as content that is created, either in whole or in part, using tools that are specific to the digital environment or is disseminated with these tools.[38] In contrast, Halbert uses a definition

[33] Rupiah K, 'Five ways to bypass social media bans' Mail & Guardian, 2 June 2016 – <http://mg.co.za/article/2016-06-02-how-to-bypass-social-media-bans/ on 16 November 2016.

[34] Rupiah K, 'Five ways to bypass social media bans' Mail & Guardian, 2 June 2016 – <http://mg.co.za/article/2016-06-02-how-to-bypass-social-media-bans/ on 16 November 2016.

[35] Bearak M, 'Shut down Zimbabwe protests are met with internet blackouts and arrests' The Washington Post, 6 July 2016 – <https://www.washingtonpost.com/news/worldviews/wp/2016/07/06/shut-down-zimbabwe-protests-are-met-with-internet-blackouts-and-arrests/ on 16 November 2016.

[36] UNHRC, *Article 19 Resolution on the promotion, protection and enjoyment of human rights on the Internet,* UN A/HRC/32/L.20 1 July 2016.

[37] Scassa T, 'Acknowledging copyright's illegitimate offspring: User-Generated Content and Canadian copyright law' in Geist M (ed) *The copyright pentalogy: How the Supreme Court of Canada shook the foundations of Canadian copyright law*, University of Ottawa Press, Ottawa, 2013, 432.

[38] Gervais D, 'User-Generated Content and music file-sharing: A look at some of the more interesting aspects of Bill C-32' in Geist M (ed) *'Radical extremism' to 'Balanced copyright': Canadian copyright and the digital agenda*, Irwin Law, Ontario, 2010, 465.

that relies upon who makes the content, rather than what the content actually is.[39] That is, UGC is used to describe activities engaged in by those not normally seen as cultural producers, but as cultural consumers.[40] Although it is certainly worthwhile to delve into the various definitions of UGC, particularly in relation to the emphasis placed upon different features, for the purposes of this essay it is acceptable to rely upon the taxonomy employed by copyright lawyers. UGC can be divided into three broad categories: content authored by users, content derived by users and content copied by users.[41] This approach emphasises the ways in which individuals engage with digital works in the digital environment. The first category could relate to reviews of products or services, blog posts, photographs and videos uploaded to social networking sites. The second category relates to new content that has been created through the modification of an existing work while the final category relates to the copying and dissemination of copyright-protected materials.[42] The rise of UGC is a result of the widespread digitisation of works, the availability of internet platforms where UGC can be shared and disseminated and the general accessibility of the software required to modify, mix and mash up digital content. That is not to say that UGC did not exist before the advent of the internet. Indeed, satire, parody, fan fictions and other forms of UGC have been around since before widespread digitisation occurred.[43] However, as a result of the ease by which users can participate, edit and disseminate such content, the digital environment has come under the legislative eye. As will be shown, one of the most important aspects of such legislation is that it is an attempt to establish a legislative basis for the regulation of content in digital form that is distributed through electronic media.

The creation of UGC has often been characterised as an economically neutral and parasitic activity.[44] This is based on the premise that UGC, by its very nature, is necessarily amateurish and carries little significance except within small or niche circles. However, the label of UGC is broad enough to capture a diverse range of activity. As noted above, fan fiction, mashups, video game modifications, and parodic works can also be considered UGC.[45] These works often reach

[39] Halbert D, 'Mass culture and the culture of the masses: A manifesto for User-Generated Rights' 11 *Vanderbilt Journal of Entertainment & Technology Law* 4, 2009, 924.

[40] Halbert D, 'Mass culture and the culture of the masses', 924.

[41] Gervais D, 'The tangled web of UGC: Making copyright sense of User-Generated Content' 11 *Vanderbilt Journal of Entertainment & Technology Law* 4, 2009, 842.

[42] Scassa T, 'Acknowledging copyright's illegitimate offspring', 432.

[43] Scassa T, 'Acknowledging copyright's illegitimate offspring', 433.

[44] Scassa T, 'Acknowledging copyright's illegitimate offspring', 434.

[45] Scassa T, 'Acknowledging copyright's illegitimate offspring', 434.

a wide audience and are of cultural significance. Of particular importance, with regard to innovation and development, is the fact that UGC also includes the broad range of works and activities as contemplated by the open data movement.[46] Individuals may utilise copyright-protected compilations of data and use them to create 'apps'. Such apps often rely upon geospatial data and the layering of other content in order to create maps or systems (such as those relating to public transit systems or 'pot hole' notification apps). Such activities have been actively encouraged by governments seeking to promote economic development and stimulate innovation.[47] Seen in this context, UGC can be innovative and useful and can make a significant social and economic contribution. Due to the broad range of activities that can be characterised as UGC and the social and cultural importance of such activities, recent steps have been made to regulate the use and creation of such content in South Africa.

V. South Africa's Film and Publication Board and the Online Regulation Policy

The Film and Publication Board (FPB) is a content-classification and censorship authority established and created under the Films and Publications Act, 1996.[48] The ostensive role of the FPB is to regulate the creation, production, possession and distribution of certain publications and certain films by means of classification.[49] One of the underlying objectives of the FPB is to protect against the sexual exploitation or degradation of children in publications, films and on the internet.[50] Until recently the FPB was predominately focused on the classification and monitoring of activities on physical platforms, and less on digital platforms and social media. The Online Policy and the Amendment Bill represent part of an effort to modernise the law in this regard. The Memorandum on the Objects of the Amendment Bill states that the increasing demands for online content and technological advances require the Board to extend its focus to the regulation of content on these diverse platforms. In this regard, it is necessary for the applicable legislation, policies and procedures to reflect these demands and technological advances.

46 Scassa T, 'Acknowledging copyright's illegitimate offspring', 434.
47 Scassa T, 'Acknowledging copyright's illegitimate offspring', 434.
48 Section 2 *Film and Publications Act* 65 (South Africa).
49 Section 2 (a), *Film and PublicationsAct* 65 (South Africa).
50 Section 2 (a), *Film and PublicationsAct* 65 (South Africa).

The FPB has published the final version of its Online Regulation Policy.[51] The draft version was incredibly ambitious and dealt extensively with UGC. UGC, in terms of the definitions of the policy, refers to any and all content created by users of online services which enable such content to be uploaded by the user. This would, in line with the definitions provided above, include blogs, wikis, forum posts, podcasts, digital images, videos and audio files. In terms of the Ellipsis overview of the FPB policy, the policy is to be interpreted to apply to both professional and amateur UGC. Moreover, in terms of the Ellipsis framework, it is not relevant whether consumers pay to view such content or not.[52] Fortunately, the FPB has realised that it would be impossible to deal with, screen and regulate all UGC and, in the Film and Publications Amendment Bill, this has been narrowed to 'specific instances' which are found to violate the provisions of the Film and Publications Amendment Bill.[53] The FPB will have the discretion to monitor and regulate instances where digital content contains sexual conduct which violates human rights, is deemed to be degrading or infringes upon the rights enshrined by the Constitution.[54] While the use of 'specific instances' and particular reference to the Constitution is more limiting than was envisaged by the draft policy, the ambit of the FPB, in terms of the Amendment Bill, is fairly broad and it has the authority to regulate any content that may advocate propaganda for war, incite violence or advocate racial hatred.[55] In terms of the Amendment Bill, the FPB may approach a media platform, internet services providers and link services and order the removal of the offending content and institute criminal charges, where appropriate.[56]

It is submitted that this is may be first step in a transition towards online censorship. This claim can be supported by the fact that the FPB would be severally limited in its ability to take action against international content providers and hosting sites. In order for the FPB to be successful in its restriction of content that does not comply with its policies and enabling legislation, the FPB would need to increase the ambit of the restrictions it wishes to implement. That is, when dealing with content from an international source that violates the Amendment Bill and its policies, the FPB would not be able to rely upon the options

51 Draft Online Regulation Policy: Film and Publication Board in GN 182 *Government Gazette* 38531 of 4 March 2015.

52 South African Communications Forum, *Submission on the draft online regulation policy*, 15 July 2015.

53 Section 18 (H), *Film and Publications Amendment Bill* (South Africa).

54 Section 1 (a) (*i*), *Film and Publications Amendment Bill* (South Africa).

55 Section 28, *Film and Publications Amendment Bill* (South Africa).

56 Section 18 (e) (2), *Film and Publications Amendment Bill* (South Africa).

listed in the above, as these will only have national application. The most effective means to prevent users from accessing such content would be to block such content, even if it originates from an international source.

Censor Walls and their Impact

Internet regulations of this sort are not particular to the African continent. Indeed, in China 'The Great Firewall' operates as a massive censorship system that assesses each internet request and decides, individually, whether or not the request should be granted.[57] Countries such as Canada, Sweden and Australia have all dealt with and maintain different forms of censorship systems.[58] Likewise, Russia has created a national censor wall that individual companies can add URLs to, with little-to-no oversight or review.[59]

In democratic nations, such initiatives invariably begin with the goal of reaffirming and establishing the *bono mores* of society in the digital environment. The protection of children, the screening of child pornography and the erasure of gratuitous violence are paramount amongst these values.[60] One of the stated initiatives of the FPB Amendment Bill is to prevent the exposure of children to harmful and gratuitous media content on the internet.[61] Nonetheless, it must be noted that censor walls do not act as an effective deterrent and can be circumvented through the use of a variety of tools, all of which are freely available on the internet. Proxies, VPNs and applications such as Tor have proven to be efficient tools to bypass censor walls and are relatively easy to use.[62] In order to prevent such an occurrence, further legislative steps would need to be taken in order to limit or prohibit access to such tools, thereby implementing further censorship laws. Such an approach is exactly what the Russian Association for the Protection of Copyright on the Internet has proposed.[63]

One of the consequences of the implementation of an effect censor wall system would be that there would be no need to censor the list of websites that

---

57 Ensafi R, Winter P, Mueen A and Crandall J, 'Analyzing the great firewall of China over space and time' 1 *Proceedings on Privacy Enhancing Technologies* 1, 2015, 61.

58 Lobato R, Meese J, 'Australia: Circumvention goes mainstream' in Lobato R and Meese J (eds) *Geoblocking and global video culture*, Institute of Network Cultures, 2016, 125.

59 Doctorow C, *Information doesn't want to be free*, 1ed, McSweeney's, San Francisco, 2015, 115.

60 Doctorow, *Information doesn't want to be free*, 110.

61 Section 16 (f), *Film and Publications Amendment Bill* (South Africa).

62 Ensafi R *et al*, 'Analyzing the great firewall of China over space and time', 65.

63 Doctorow, *Information doesn't want to be free*, 111.

have been blocked. As the public would not be able to access them, this would be unnecessary. Because this is not the case, however, the publishing of a list of blocked websites and domains would defeat the purpose of the censor wall system.[64] Those who have access to the tools to circumvent the censor wall would be able to access any of the sites on the list with relative ease. As a result, such a list of 'prohibited sites' would need to be made inaccessible to the general public. In cases relating to obvious abuses—such as child pornography and violence—this would be relatively easy to justify. However, this would be to assume that there are not more things that the governments and their agencies would like to suppress. Content relating to extreme political beliefs, drug legalisation advocacy, euthanasia, mature pornography and websites that allow for the download of copyright infringing material may quickly be included in this block list.[65] Moreover, issues relating to piracy and copyright abuse may become relevant as censorship offers an easy, if not particular effective, means to curb such practices. The problem here is that it is incredibly difficult to tell, from a cursory examination of most websites, whether the content does in fact infringe upon the rights of the copyright holder. Even if the content has been uploaded with the permission of the copyright holder, it may still fall under one of the various copyright exceptions and, as a result, not constitute an infringement.[66] Such issues are best left to the courts to determine as they are better equipped to make such decisions. As these examples have illustrated, issues of abuse and infringement can become complicated and, in such instances, it is not unlikely that much content will simply be blocked until the issue is raised in court.

While the measures taken by the FPB are tentative, they have the potential to cause traumatic consequences for South Africa. The governing and regulation of online content and the positive enforcement measures taken to ensure that such measures are successful may lead to the infringement of various human rights and provide the State with an opportunity to deny access to any content it considers unsuitable for the public. Such a task was once considered best left to parents and families.[67] Simply put: by blocking and censoring illegal or unregulated content, the State's legislative body takes steps that will inevitably limit free speech and expression on the internet. The consequences of an overarching internet regulation are not limited to the financial sector. In 2012, in Russia, an

64 Doctorow, *Information doesn't want to be free*, 111.

65 Doctorow, *Information doesn't want to be free*, 111.

66 Section 12, *The Copyright Act* (South Africa).

67 Wong Y, Ho K and Chen H, 'Internet supervision and parenting in the digital age: The case of Shanghai' 7 *The Open Family Studies Journal* 1, 2015, 113.

internet law with motivations not unlike the FPB's went into effect. Its purpose was to protect children from websites that promoted drug use, suicide and paedophilia.[68] The Act established a blacklist of websites that were prohibited. The list was updated daily and each website was either shut down or blocked entirely.[69] The Act was heavily criticised, both abroad and in Russia, and many argued that the law was simply a means to curb freedom of expression.[70] Although these arguments were met with assurances, in the following weeks the government began to implement the bans in order to suppress criticism from opposition leaders and groups.[71] These websites included satirical pages that mocked Vladimir Putin and Russian officials.[72] While both democratic and non-democratic nations have moved towards greater regulation, it is clear that it is the authoritarian regimes that have implemented the most stringent of regulations.

VI. The Regulatory Framework: The Cybercrimes and Cyber Security Bill

The FPB's Online Regulation Policy forms part of a series of new proposed cybercrime policies and laws that are being drafted in South Africa. Another important piece of legislation relating to ICTs is the Cybercrimes and Cyber Security Bill.[73] The Bill has been overshadowed by criticism and, while the legislation has not yet been implemented, some believe that this law would be excessive.[74] Some of the criticism is a result of the fact that the Bill includes a number of the deeply flawed provisions of the Protection of State Information Bill. The Protection of State Information Bill has been notoriously dubbed the 'Secrecy Bill' and, at the time of writing this paper, had been passed by the National As-

68 Kerr J, 'The digital dictator's dilemma: Internet regulation and political control in non-democratic states' Published PhD Thesis, Stanford University, California, 2014, 2.

69 Elder M, 'Censorship row over Russian internet blacklist' The Guardian, 12 November 2012 – <https://www.theguardian.com/world/2012/nov/12/censorship-row-russian-internet-blacklist on 17 November 2016.

70 Ognyanova K, 'Careful what you say: Media control in Putin's Russia – Implications for online content' 1 *International Journal of E-Politics* 2, 2014, 19.

71 Ognyanova K, 'Careful what you say', 20.

72 Kerr J, 'The digital dictator's dilemma: Internet regulation and political control in non-democratic states' Published PhD Thesis, Stanford University, California, 2014, 2.

73 Section 58, *Draft Cybercrime and Cybersecurity Bill* (South Africa).

74 Rawlins K, 'SA cybersecurity laws must be 'modernised" IT Web Security, 6 July 2016 – <http://www.itweb.co.za/index.php?option=com_content&view=article&id=154038:SA-cyber-security-laws-must-be-modernised-&catid=234> on 17 November 2016.

sembly. As such, all that remained was for the President to sign it so that it could become law.[75] However, due to threats of a challenge in the Constitutional Court, it had remained unsigned for over two years.[76] Unfortunately, the Cybercrimes and Cyber Security Bill seems to be an attempt to push through certain aspects of the Secrecy Bill and, while policies that promote online security and the safety of ordinary citizens are necessary, critics say that the Bill operates to threaten and curb internet and journalistic freedom.[77]

From the outset it becomes clear that the Bill suffers from a number of problems. Paramount amongst these is the fact that the Bill places the internet firmly under the control of the Ministry of State Security.[78] This follows a trend which, in recent years, has seen internet policy and security transferred from the organs of state responsible for promoting access to communication and information to the Ministry of State Security.[79] The problem herein lies with the fact that the Ministry of State Security lacks the necessary accountability, civilian oversight, transparency and organisational culture appropriate for such a task.[80] This may be illustrated by the fact that a previous version of the Bill was deemed to be a classified state document until 2015.[81] This shifting and expanding role for South Africa's state security structures, while potentially dangerous, also contradicts the narrowly defined and regulated role envisaged by the Constitution.[82] The Bill would operate to create a set of new agencies and structures with wide-ranging powers. Such powers would be used to introduce and shape policies and

---

75 Evans S, 'Opposition hopes for secrecy Bill court review' Mail & Guardian, 25 April 2013 – <http://mg.co.za/article/2013-04-25-will-the-secrecy-bill-go-to-the-concourt> on 17 November 2016.

76 Evans S, 'Opposition hopes for secrecy Bill court review' Mail & Guardian, 25 April 2013 – <http://mg.co.za/article/2013-04-25-will-the-secrecy-bill-go-to-the-concourt> on 17 November 2016.

77 Joseph R, 'South Africa's Cybercrimes and Cybersecurity Bill is deeply flawed' Index on Censorship, 7 January 2016 – <https://www.indexoncensorship.org/2016/01/raymond-joseph-south-africa-cybercrimes-and-cybersecurity-bill/> on 10 June 2016.

78 Joseph R, 'South Africa's Cybercrimes and Cybersecurity Bill is deeply flawed' Index on Censorship, 7 January 2016 – <https://www.indexoncensorship.org/2016/01/raymond-joseph-south-africa-cybercrimes-and-cybersecurity-bill/> on 10 June 2016.

79 Right to know, 'R2K submission on draft Cybercrimes and Cybersecurity Bill' Right to Know Publications, 30 November 2015 –<http://www.r2k.org.za/2015/11/30/cybercrimesbill/> on 16 November 2016.

80 Joseph R, 'South Africa's Cybercrimes and Cybersecurity Bill is deeply flawed' Index on Censorship, 7 January 2016 – <https://www.indexoncensorship.org/2016/01/raymond-joseph-south-africa-cybercrimes-and-cybersecurity-bill/> on 10 June 2016.

81 Joseph R, 'South Africa's Cybercrimes and Cybersecurity Bill is deeply flawed' Index on Censorship, 7 January 2016 – <https://www.indexoncensorship.org/2016/01/raymond-joseph-south-africa-cybercrimes-and-cybersecurity-bill/> on 10 June 2016.

82 Article 6 *White Paper on Intelligence* (South Africa).

standards for the internet in South Africa.[83] Moreover, these agencies would have the power to declare any data, database, device, network or infrastructure to be a 'National Critical Information Infrastructure'.[84] This would apply to assets which are both publicly or privately owned and, effectively, allows for the state-security network to lay claim to any part of the internet and declare it to be an asset crucial to national security.[85] An overwhelming majority of these agencies would report to the Ministry of State Security.[86]

i) The Existing Framework: Surveillance and Constitutional Issues

The existing surveillance law found in the Regulation of Interception of Communications and Communication-related Information Act (RICA) would operate parallel to the Bill.[87] RICA has been heavily criticised on a number of grounds.[88] Notably, the vagueness of many of the provisions, the lack of transparency and the restrictions placed upon telecommunications companies and internet service providers are cause for concern.[89] Moreover, users under surveillance are not notified of warrants granted to intercept their data, even after the fact. Aside from the designation of power and duties, the Bill itself provides surveillance powers that, without adequate checks and balances, may prove to be invasive. The Bill, coupled with the existing surveillance law found in RICA, creates the opportunity to go beyond the mere interception of data that is an indirect communication or real-time communication and can be applied to the interception of almost any possible data that might exist.[90] Section 26 of the draft Bill provides that its invasive powers may be exercised to access information connected to any offence. In terms of the section, investigators, with unspecified characteristics and who are not public officials, are given significant powers to investigate such offences. Another criticism which may be levelled against the Bill is that the Bill delegates significant powers to magistrates to authorise the interception of communications.[91] Such a provision ignores the fact that magis-

83 Section 58, *Draft Cybercrime and Cybersecurity Bill* (South Africa).
84 Section 58, *Draft Cybercrime and Cybersecurity Bill* (South Africa).
85 Section 58, *Draft Cybercrime and Cybersecurity Bill* (South Africa).
86 Section 51, *Draft Cybercrime and Cybersecurity Bill* (South Africa).
87 *Regulation of Interception of Communications and Communication-related Information Act* (South Africa).
88 Luck R, 'RICA: Walking a fine line between crime prevention and protection of rights' *De Rebus*,2014, 31 —<http://reference.sabinet.co.za/document/EJC147838> on 18 November 2016.
89 Luck R, 'RICA: Walking a fine line between crime prevention and protection of rights' *De Rebus*,2014, 31 —<http://reference.sabinet.co.za/document/EJC147838> on 18 November 2016.
90 Section 39 (2), *Draft Cybercrime and Cybersecurity Bill* (South Africa).
91 Section 40 (6), *Draft Cybercrime and Cybersecurity Bill* (South Africa).

trates may not be best suited to handle such matters and may not have sufficient expertise in the law relating to communications surveillance, the technology used and the human rights issues concerned.

In an effort to create a balance between freedom of speech and the regulation deemed necessary to ensure that the internet does not become a platform for language and expression that is deemed *contra bonos mores*, the Bill introduces a number of criminal offences. Section 17 of the Bill creates a set of criminal offences for anyone who 'makes available, broadcasts or distributes… a data message which advocates, promotes or incites hate, discrimination or violence against a person or a group of persons'.[92]The Bill provides further clarification by stating that the above should be understood as any data message representing ideas or theories, which advocate, promote or incite hatred, discrimination or violence, against a person or a group of persons, based on (a) national or social origin; (b) race; (c) colour; (d) ethnicity; (e) religious beliefs; (f) gender; (g) gender identity; (h) sexual orientation; (i) caste; or (j) mental or physical disability.[93] Although, *prima facie*, these restrictions and the criminal sanctions that follow the violation of these provisions seem to be reasonable, they go beyond the limitations on freedom of expression provided for in Section 16 (2) of the Constitution.[94] In terms of this provision, freedom of expression does not extend to 'advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm'.[95] In terms of the Constitution, hate speech only occurs if a message contains an incitement to cause harm. Moreover, a further requirement is that such a message advocates action to cause harm on the grounds of ethnicity, race, gender or religion. Although well meaning, the provisions of the Bill go beyond these limits and, as a consequence, constitute an infringement on the constitutionally protected right to free speech.[96]

Section 18 of the Bill is also problematic as it makes it an offence for anyone to make available, broadcast or distribute 'a data message which is reasonably likely to incite: (i) violence against (ii) damage to the property belonging to a person or a group of persons'. This applies to messages sent to a single person or to the general public and, as is the case with Section 17, is based upon too

92 Section 17 (1) (c), *Draft Cybercrime and Cybersecurity Bill* (South Africa).

93 Section 17 (3), *Draft Cybercrime and Cybersecurity Bill* (South Africa).

94 *Constitution of the Republic of South Africa*, 1996.

95 *Constitution of the Republic of South Africa*, 1996.

96 Joseph R, 'South Africa's Cybercrimes and Cybersecurity Bill is deeply flawed' Index on Censorship, 7 January 2016 – <https://www.indexoncensorship.org/2016/01/raymond-joseph-south-africa-cybercrimes-and-cybersecurity-bill/> on 10 June 2016.

broad an interpretation of the restriction on freedom of speech.[97] The Constitution prohibits the incitement of imminent violence and not violence in general. Moreover, it does not explicitly restrict damage to property at all.[98] As a result, these provisions may operate to cause constitutionally indefensible censorship of internet content and data. Despite the fact that the Department of Trade and Industry is already undertaking amendments to South Africa's copyright law, Section 20 of the Bill provides criminal penalties for a number of offences which relate to copyright infringement. As with RICA, this creates the situation where two separate pieces of legislation run parallel and creates the opportunity for vagueness and the restriction of user rights.

ii) Regulation and Its Consequences

The delivery of internet content to the general public requires a number of independent actors. Authors, publishers, telecommunications operators and internet access providers all operate within a highly technical field and, essentially, a borderless environment. Over-regulation and imprecise laws create confusion among these various actors, which leads to uncertainty among users. Unnecessary regulation of the internet creates both legal and operational barriers for businesses and investors. This inhibits economic development and hampers growth while favouring well-established manufacturers over new competitors. As a result, competition is hindered and the potential for a competitive market is reduced. When restriction and regulation is required, it should be narrowly defined and implemented. This limits the potential for uncertainty and ensures that growth and development are not seriously hindered. In the developing world this becomes even more important. Regulatory ambiguity, short sightedness or inadequacy can cause investors to shy away from investing in new internet start-ups and already established businesses that wish to expand their market.[99] A 2014 study has shown that governments in developing countries, such as South Africa, need to do more to ensure that regulation and policies do not inhibit investment in the field of ICTs.[100] The study found that, while regulation is necessary, investors are most concerned about regulatory ambiguity.[101] The study related to

97 Section 18, *Draft Cybercrime and Cybersecurity Bill* (South Africa).

98 *Constitution of the Republic of South Africa*, 1996.

99 Le Merle M, Davis A and Le Merle F, *Fifth Era:The impact of internet regulation on early stage development,* 2014, 16.

100 Le Merle M *et al*, *Fifth Era: The impact of internet regulation on early stage development,* 2014, 17.

101 Le Merle M *et al*, *Fifth Era: The impact of internet regulation on early stage development* 2014, 23.

thirty SA-based investors who all stated that the current policy environment in the technology sector had had a negative impact on their investment activities.[102] The issue, it is submitted, is not the impact a single piece of legislation or proposal will have but, rather, the accumulated impact they will have upon the digital environment.

VII. Conclusion

It seems that, despite the many steps made in recent years, South African legislation, in force and proposed, fails to ensure that the delicate balance between regulation and freedom of expression is maintained. Moreover, if future drafters do not take cognisance of the dangers that such stringent regulation and criminalisation pose, it is likely that innovation and expansion within the domain of the digital environment will be curtailed. The future of South African information and communication technologies will depend upon a number of factors. First, unity and a single policy based approach by the various departments will ensure consistency and that a more efficient system is maintained. Secondly, the many criticisms of those who have been charged with the examination of our system should be taken into account when policy is adopted or legislation drafted. Finally, in order for a consistent and well run regime to govern the digital environment, the drafters of such legislation and policies will need to refer to the well-established democratic and human rights norms. The potential for harm an unregulated environment may cause is obvious. However, overcompensating with the unjustifiable limitation of constitutional rights and the diminishment of internet freedoms is a threat to the principles of democracy and not an alternative we should consider.

[102] Le Merle M *et al*, *Fifth Era: The impact of internet regulation on early stage development* 2014, 20.