Human Rights and Information in Africa: A reflection on trends

By Gabriella Razzano

fesmedia Africa series
2016

FRIEDRICH EBERT STIFTUNG

Published by fesmedia Africa, Friedrich-Ebert-Stiftung
P O Box 23652
Windhoek, Namibia
Tel: +264-61 417 500
Email: info@fesmedia.org
www.fesmedia-Africa.org

ISBN: 978-99945-77-34-7

---

fesmedia Africa
fesmedia Africa is the media project of the Friedrich-Ebert-Stiftung in Africa. With our partners in civil society and politics, fesmedia Africa furthers media freedom, the right to information, an independent media, and the diversity of media content in support of good governance, democratisation and socio-economic development.

FES in Africa
With offices in 19 Sub-Saharan African countries the Friedrich-Ebert-Stiftung promotes democratisation, good governance and social development in cooperation with partners in politics and society.

Friedrich-Ebert-Stiftung
The Friedrich-Ebert-Stiftung (FES) is a non-governmental and non-profit making political foundation. FES is represented in around 100 countries throughout the world. Established in 1925 the FES is committed to the ideas and basic values of social democracy - political participation, social justice, and solidarity – to preserve the legacy of Germany's first democratically elected president, Friedrich Ebert.

Human Rights and Information in Africa:
A reflection on trends

By Gabriella Razzano

2016

Contents Page

Introduction

One in three people on the planet is an Internet user.[1] It has emerged as a new lived space and reality for citizens, and thus also a new space in which human rights has to be considered. In the early days of the Internet, many hoped it would be an almost regulation-free utopia. The reality of the modern world however is that regulation is inevitable. The question then becomes: are the trends in regulation advancing human rights, or negating them on the African continent?

The 'Internet' is often treated as an alien space for human rights concerns, which is why the debate is often limited to the right of *access*. Practically, however, the existing human rights framework is fully capable of dealing with the dilemmas that may apply online. Frank La Rue stated in his seminal commentary:

> …the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet.[2]

He also noted that the value of the Internet extended beyond just access to broadband, but also to the preservation of the Internet as a space for the creation and dissemination of content as well. The issue of content itself being worthy of human rights protection (and consideration) is important, for when people speak of a 'right to the Internet', they do so without expanding to a variety of impacts of innate concern to human rights activists, such as the preservation of the Internet as jurisdiction for enabling freedom of expression, or preserving privacy.

Bearing this in mind, we hope to look at the evolving world of human rights: new threats and new opportunities emerging on the African continent as a result of the modern age. It is always a challenging exercise to pin down developments in an area that changes so quickly, but we will nevertheless attempt to do so – by first examining phenomena in the area of Internet content, and then in the area of Internet access.

Content

Introduction

We can almost consider the Internet as a new jurisdiction. When we consider it as a physical space, it becomes easier to imagine how there are rights implications that happen within the space itself, and also when people are inhibited from entering or exiting that space. These kinds of blocks can be because of who you are, or because there are physical impediments ('locked doors'), which arise because of policy intervention or infrastructure issues. We will reflect on these are the emerging trends on access later. There are also content related issues, which relate more directly to our existing human rights frameworks in Africa. It is important to always bear in mind that, due to the nature of human rights, many of the 'categorisations' in both of the broader sections of this piece will conceptually overlap. This is quite simply because rights are mutually reinforcing and inter-connected.[3] However, systematic categorisation helps us to explain trends clearly, while indulging the overlaps in the process.

Freedom of Expression

The Internet is a vital new platform for allowing free expression. Freedom of expression is protected in Article 9 of the African Charter on Human and People's Rights:

> … 2) Every individual shall have the right to express and disseminate his opinions within the law.

In *Sconlen & Holderness/Zimbabwe* the African Court on Human and Peoples' Rights noted:[4]

> When the Charter proclaims that every individual has the right to receive information and disseminate opinions, it also implicitly emphasises the fact that the expression, reception and dissemination of ideas and information are indivisible concepts. This means that restrictions that are imposed on dissemination represent, in equal measure, a direct limitation on the right to express oneself freely.

Such a broad, and necessary, understanding of freedom of expression by African courts would clearly identify that the Internet as a platform and means for expression worthy of protection in the correct circumstances. Limits on access restrictions, but also content restrictions, are all concerns. Freedom of expression is vital for ensuring a diversity of views, accountability of those in power, and the independence of people alongside the free flow of ideas.

In Africa, one of the most direct examples of hindrances to freedom of expression is the act of physically shutting off access to the Internet. While there are some justifiable limits to rights (some of which will be reviewed later) the *Joint Declaration on Freedom of Expression and the Internet*, importantly endorsed by the three rapporteurs on Freedom of Expression from the United Nations, Organisation of American States and the African Commission on Human and People's rights, stated expressly:

> [c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting off the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet.[5]

This statement was a very real reaction to the Egyptian government shutting down access to the Internet during the 'Arab Spring', which was coupled with several other restrictive acts, such as shutting down mobile phone networks in Cairo, and also utilising SMS services to spread pro-government propaganda.

Another area of increasing concern is the forced removal of content. In this scenario, states force the removal of specific content – and impinge on freedom of expression – either through laws or intimidation. This is done in preference to filtering out that content, as the state often does not have adequate control of the content provider to enable restriction in any other way.[6] In a 2015 assessment, it was noted that there has been a significant increase in regulations (42 out of 65 of the assessed countries) requiring content of a political, social or religious nature to be removed.[7] Laws that criminalise forms of online speech reinforce this trend. In The Gambia in 2013, the Information and Communication Amendment Act was passed, specifically targeting forms of online speech, with a maximum jail term of fifteen years for statements spreading 'false news' about the government or public officials, caricatures or making derogatory statements against public officials, and/or incitements of dissatisfaction or instigating violence against the government.[8] The Act forms part of a broadly oppressive environment on freedom of expression in The Gambia.[9]

The media can be seen as important agents of free expression, and the Internet and Communications Technologies (ICT) have provided an interesting area of both opportunity for, but also threats to, traditional 'news'. From a rights perspective, attempts by states to clamp down on new media can be seen as a notable freedom of expression concern. Bloggers and online journalists are increasingly relevant media agents for many members of the public. However, alongside traditional media harassment, these new expression agents have been subject to unduly harsh treatment by states. In Ethiopia, for example, 2014-2015 saw increasingly repressive actions taken against online journalists and bloggers:

> The Zone 9 bloggers arrested in April 2014 were charged with terrorism in July 2014 and subsequently subjected to a series of sham trials through mid-2015. In July 2015, two of the imprisoned Zone 9 bloggers were unexpectedly released and acquitted of all charges, which observers attributed to U.S. President Barack Obama's official visit to the country later that month. The four remaining Zone 9 bloggers were acquitted in October. Nevertheless, five other critical voices and bloggers who were arrested in July 2014 and charged with terrorism remain in prison. During the numerous Zone 9 trials throughout 2014–2015, several supporters were temporarily arrested for posting updates and pictures of their trials on social media via mobile devices.[10]

Despite these threats, online media is of growing significance on the continent. The Internet provides a platform for massive engagement, accessible by people who may ordinarily have been removed from popular discourse. While the digital divide raises our awareness to concerns about how language can exclude people from accessing content (discussed in more detail later), it may at the same time be used to advance indigenous cultural expression if the issues around access can be engaged.

The online space also presents particularly useful tools to journalists for advancing journalism – the rise of open data journalism allows investigative journalists to harness open data for revealing and pertinent news (discussed in more detail later).[11] Online marketing strategies and social media platforms can be used effectively and cheaply to broaden a journalist's online audience – and must be considered, within the African context, given burgeoning mobile connectivity. Also, social media can facilitate debate with audiences, as there is a degree of anonymity that encourages participation. There are also strategies to offset some of the security risks endemic to working online for journalists and citizens, for example, anonymous browsing can be facilitated

through the simple and free installation of the 'Tor' software, which can be used to allow for unmonitored research.[12]

Freedom of expression is not unfettered. Rights can be justifiably limited, and freedom of expression in particular has specific limitations in relation to hate speech and speech that incites violence, throughout the African continent. The International Covenant on Civil and Political Rights (to which several African states are signatories) in Article 20, precludes any advocacy to the incitement of violence, though not expressly only within the context of speech. Commonly referred to as hate speech, this form of 'expression' is viewed as too harmful to be justifiably free. As Pierre De Vos noted:

> [Hate] speech has no value. It does not enlighten. It does not help us to think critically about how better to live in the world.[13]

Hate speech is very relevant within the online space, as social media and online forums can be havens for hate speech – fuelled by the anonymity of the forum. There has been a notable gender crisis in the abuse of women perpetuated through the Internet – through the use of threatening language, imagery and other forms of harassment. The perceived 'neutrality' of the web is in many ways farcical: 'some users are more equal than others'.[14]

There are a variety of ways in which hate speech is specifically exercised against women online – one legal review discovered that 90% of 'revenge porn' cases (where intimate photographs are publicly circulated to shame the victim) are perpetuated against women. Another study noted that 89% of domestic violence programs reported victims experiencing some form of technology-based abuse. Female staff of the website 'Jezebel' wrote an open letter to their parent company, requesting the development of blocking tools against specific Internet Protocol addresses, to assist with the deluge of sexually violent posts placed to harass users.[15] What is disturbing is that these technologies in fact help 'to increase violence against women, not just mirroring it'.[16] And laws are often slow to adapt to these new threats to the human rights of citizens. The nature of such a space complicates attempts at legal intervention:

> …a multiplicity of different actors could be involved in the creation and dissemination of hateful content: creating or sourcing it; publishing it; developing it; hosting it or otherwise facilitating its dissemination, accessibility or retrievability.[17]

On the other hand, freedom of expression is not just about media and speech, as it also includes consideration of personal or self-expression. Online and virtual spaces are forums for self-expression, and an interesting segue in this area has been considering how the law can regulate virtual worlds and characters created for online gaming, while respecting free expression.[18] The question must become: How can the law adapt to such alien environments within a human rights framework?

> What happens in virtual worlds, however, has real-world effects both on players and non-players, and governments will have important interests in regulating those real-world effects for reasons that are unrelated to the suppression of free expression.[19]

Leading from this, legal intervention in the online space should not automatically be considered a violation, as it may be necessary for the protection of the fundamental rights we hold most dear.

Access to Information and Open Data

Information is the lifeblood of the Internet. At its simplest, it can be described merely as a mechanism for electronically distributing information across distance. The right of access to information is of profound import in this space – and of profound import for development and empowerment on the African continent. When we look to standard rights instruments, there have been traditionalist tendencies to articulate access to information as an aspect of the general guarantee of freedom of expression; a legacy of the 1949 United Nations Declaration of Human Rights.[20] However, access to information has come to be recognised as a self-standing right within individual Constitutions,[21] international human rights court decisions[22] and international instruments. Of particular relevance to our purposes are the regional instruments which do so, such as Article 9 (1) of the African charter on Human and Peoples' Rights:

> Every individual shall have the right to receive information.[23]

The position makes sense given the profoundly independent value the right holds. Access to information empowers citizens to act on their rights, whilst holding governments, and the powerful, to account. Accountability is of extreme importance when we consider what a just world should be like, and the ability of access to information, pursued through the Internet, to act as a positive disruptive force has been well noted:

> The Internet has effectively returned more power to individuals with a radical redistribution of control of information flow and a completely new approach to how society operates.[24]

As a right, access to information is increasingly relevant within the African context. The post-2015 Development Agenda resulted in the production of the Global Sustainable Development Goals (SDGs) for 2030, and places access to information and the pursuit of transparency at the centre of many of the goals, whilst also envisioning the Internet as a vital role player in the achievement of these goals. [25] It has been noted within this context:

> It is self-evident that such access to information is not only a target – an aspiration and an outcome, in other words an 'end' of development. It is also a means towards achieving all the other targets of development, and not least those on justice, health, education, environment and gender.[26]

There is also an active access to the information movement spanning the continent. In 2015, UNESCO adopted a Right of Access to Information Day, on 28 September, as a result of African lobby groups, and at the proposal of African delegations. While there are still many African countries that need to adopt a specific access to information law, seventeen countries currently do so (up from only five in 2010).[27] Pertinently, the African Declaration on Internet Rights and Freedoms in Article 4 states:

> Everyone has the right to access information on the Internet. All information, including scientific and social research, produced with the support of public funds, should be freely available to all, including on the Internet.

The right of access to information is not only about information in the form of research. Information would include data. Open data is a peculiarly special opportunity for information activists within the online space. Open data represents a form of proactive disclosure of information. Government is the largest custodian of information – from service delivery agreements, to service maps, to border surveys and water quality reports. Most of these types of information have no justifiable reason for being kept from the public and, with the heavy bureaucratic burden that access to information laws can place on public bodies, need not require a request in order to allow citizens access,

but can be openly provided instead. Opening up government information has a direct benefit for the state, and a significant benefit for citizens. Not only does it improve their access to information, but it also creates opportunities to translate that data more easily into information that has value for people, such as in interactive applications, or summarising printed information sheets. It can even create job opportunities; there are many creative ways that open data can be used to support business innovations, particularly in the mobile applications market.

The open data movement has a notable history in Kenya, and the country was often cited as a regional leader after launching an 'early' government open data portal in 2001 (although Morocco preceded its actual launch). In some ways, inspired by this initiative, the open data movement in Kenya is also significant, with hubs such as iHub being centres for open data innovation. However, the quality of the data released has often been criticised and their open data projects, while providing usefully compressed information, are failing to have significant impact for grassroots communities.[28]

Of greater concern has been the inability of the Kenyan government to pass a specific access to information law. This raises an important issue: the problem of 'open washing'. This problem notes that sometimes when a government is being open with data, this data is not necessarily enough to hold the state to account. From a political perspective, a government may be willing to forward data, as it controls release – but may nevertheless hesitate to permit access to controversial data demanded for by citizens which enhances real accountability. This is why access to information laws remain important.

The Open Government Partnership is an influential multilateral initiative in this area that aims to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption and harness new technologies to strengthen governance. Governments who sign the Open Government Declaration pledge commitments to 'stretch government practice beyond its current baseline', that are then implemented by the state, and peer monitored. These include open data and access to information commitments. Importantly for the region, South Africa will be Chair of the Steering Committee in 2016, though only nine African countries have signed the Declaration. It is clearly an area of opportunity for activists moving forward. Open data is central to the 2030 Sustainable Development Agenda, and the

spread of information is of central importance throughout. Of particular note in this regard is paragraph 48, which states:

> Indicators are being developed to assist this work. Quality, accessible, timely and reliable disaggregated data will be needed to help with the measurement of progress and to ensure that no one is left behind. Such data is key to decision-making. Data and information from existing reporting mechanisms should be used where possible …

This speaks not only of the necessity of open data, but also as to how open data can be a clear catalyst for a type of networked thinking that integrates various strands of activity.

Good Governance

For a state to govern well, it must do so transparently and accountably. Good governance is a term that stands as a catchall for human rights ambitions that look to create the correct political environment for development. Rights such access to information, the right to participate in political affairs, and the right to freedom of expression all contribute to good governance. Corruption fighting activities are vital for effective state functioning and are an incredibly significant problem on the African continent.

An interesting way of defining corruption was made by Klitgaard in the creation of this formula:

Corruption = Monopoly Power + Discretion – Accountability.[29]

The example of South Africa is instructive in this area. In South Africa, a newspaper or news site seemingly cannot pass a day without corruption and mis-expenditure seizing at least one headline. It has been estimated that R700 billion has been lost to corruption over the last 20 years by the Institute of Internal Auditors. Yet, the Open Government Index ranked South Africa's performance as fairly strong in terms of that index. Internationally, South Africa ranked as the 27th most 'open government' out of the 102 countries evaluated, and the highest ranked African country regionally.[30] Comparatively, in the public perception index from Transparency International's Corruption Perception Index[31] South Africa has not been faring well, as in 2014 they were ranked 67th out of 175 countries on the corruption scale, with several African countries being perceived as notably less corrupt. The results seem somewhat inconsistent. Yu and Robinson in 2012 noted that open government should

not be conflated with open government data, as open government is more than just being open about information; it is also about being open about information that forwards accountability.[32] Thus, if the information being provided is not accountability information, corruption can still thrive.

In the fight against corruption, the role of the whistleblower is vital. Studies have demonstrated that whistleblowing is the most effective method for detecting fraud and corruption.[33] Yet many countries have ineffective and weak protections for whistleblowers. Whistleblowing, and the online environment, have in the main senses become synonymous, fuelled by the ease of which disclosed information can be disseminated online.

One of the most famous cases of repression of the online whistleblower is the American case of Edward Snowden who, in 2013, revealed to the world the various National Security Agency programs that were (and are) unjustifiably infiltrating civilian lives and data.[34] Snowden has since been living in exile, in fear of arrest for various contraventions of disclosing 'classified' information and espionage charges. Yet, in spite of the prevalence of victimisation of whistleblowers, protection should be in place for legitimate disclosures, and with the G20 noting statute, should:

> … clearly [define] the procedures and prescribed channels for facilitating the reporting of suspected acts of corruption, and [encourage] the use of protective and easily accessible whistleblowing channels.

While several African countries have whistleblower protection laws, Ghana has also instituted a statute that allows for financial incentives. The Ghanaian Whistleblower Act 270 of 2006 appears to have been one of the first specifically legislated financial incentive systems for whistleblowers in Africa. The law created a central and dedicated fund called the Whistleblower Reward Fund, created from contributions and specific allocated amounts from Parliament. The fund can be accessed to reward a whistleblower "who makes a disclosure that leads to the arrest and conviction of an accused person".[35] Further, if a disclosure leads to money being recovered, the whistleblower will receive a percentage of the funds.[36] This is a proactive method of incentivising whistleblowers, and also helps compensate against the real financial consequences for whistleblowers when they make disclosures.[37]

The Internet may be a mechanism for assisting secure whistleblowing. An example of such an initiative is Afrileaks.[38] The site allows for the secure leak of

documents that have a public interest. These are then provided to journalists who can authenticate and expand on the content.

Personal Privacy

Personal privacy is the human rights idea that considers an individual's personal life an area of sanctity, worthy of rights protection. Looking at classical human rights enunciations, the Universal Declaration of Human Rights refers in Article 12:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

There is a strong link between the private space and the person in the quotation above. However, in the Internet age, privacy has become a particularly notable area of concern in relation to the protection of a person's own data.

Interestingly, the right to personal privacy was not expressly included in the African Charter on Human and Peoples' Rights, although it is often domestically protected. However, several African countries including Nigeria, Tunisia and Ghana specifically recognised the United Nations Human Rights Commissioner's resolution on 'privacy in the digital age'.[39] This resolution was a response to the perceived increased use of technology by states for the surveillance of citizens, and the interception of personal communications. It recognised both the opportunity that ICT's provide for development and the enabling of rights, but also called on states to take steps to put an end to the violation of rights, unlawful surveillance and interceptions of data. ICT's can be used with great utility to diminish the 'systemic risks' associated with the media revolution, such as those to personal privacy, but can also be used to violate them.[40]

The Internet has the power to transfer huge amounts of data, but blanket collection of data also makes for easier interception. Metadata has become a buzzword of importance in this field – and is probably most easily explained as 'data about data'. It is the packets of information that go alongside a piece of data, which can help identify the source, and can thus expose a person's privacy if collated. As we noted earlier, Edward Snowden alerted the world to the mass surveillance of civilian data by the United States – but many countries to appear guilty of this. While often there are laws that may allow for

justifiable surveillance, which intrudes on citizen privacy, domestic regulation on communications interception has been abused as well. For instance, an American citizen of Ethiopian descent sued the Ethiopian government in 2014 for violations after realising he was being surveilled.[41] African governments have also participated in mass surveillance alongside the United States of America, with several states cited as having procured mass surveillance technologies by popular German producer Trovicor.[42] The Egyptian government has frequently been outed for the mass surveillance of social media communications through its 'Social Networks Security Hazard Monitoring Operation'.

Another thematic area of concern is encryption and states attempting to regulate in this area. Encryption is used to secure a person's transactions and communications online. It is a very practical mechanism for ensuring privacy. However, states which attempt to regulate encryption can impinge on this privacy. A report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, noted in 2015 that over-regulation in this area can directly violate on an individual's privacy rights.[43] In Ethiopia, for example, the state is empowered to set the technical standards of encryption, and has enacted regulation that criminalises the manufacture, assembly or import of any telecommunications equipment without a permit.[44] This appears as a clear infringement of human rights.

A further example of the intersection of ICT's and the right to privacy is the somewhat controversial, and potentially misguided, judgment of the European Court of Justice and the 'right to be forgotten'. While not a right contained in the Universal Declaration on Human Rights or the African Declaration on Human and Peoples' Rights, the court held under the auspices of the right to privacy, that the right to be forgotten exists. This means that search engines can be ordered to remove content from their indexes (even though they have nothing to do with its creation) by individuals that have applied for a court order.[45] However, the right to be forgotten has never been a right in history,[46] and the guidelines for when such orders must be complied with are vague. As one critique noted:

> This is the kind of endless whack-a-mole game that comes about when governments use blunt instruments to censor the internet. It's a sad fact that content on the internet lives forever — or until the organization hosting it takes it down, at least. Asking Google to remove that content from its search engine is akin to asking libraries to remove news stories about individuals from their archives.

Privacy is a right, and impositions on privacy and personal data can have a negative impact, not only on the personal sphere of the individual, but also on the 'free development and exchange of ideas'.[47]

National Security and Cyber Security

National security is a regulatory sphere increasingly used by states to justify limitations on human freedoms. This is all within a context that notes:

> National security is … one of the most difficult areas for campaigners and human rights activists to promote reform, both politically and through the courts.[48]

The two issues need not be set up as opposition, although in practice they have been. There have been direct attempts to reconcile the two concepts through work on 'human security', in other words, moving the focus away from the state and considering security as necessary for the preservation of an individual's rights. These debates aside though, it is worth considering national security and cyber security as an important trend on the continent.

Contextually, in many countries the 'securocrat' is on the rise, resulting from the principles of national security being established as the priority agenda throughout *all* administrative functions. This leads to threats of increased secrecy across the policy board from a new range of government actors acting as state security officials in their ordinary functions.[49] This stands as a threat to information access and good governance.

When we consider the issue of national security in respect of rights such as freedom of expression and access to information, there have been many instances where the concept has led to abuse. We can consider, for example, the attempts made by the South African government to pass the Protection of State Information Bill.[50] While the stated intended purpose of the law was to reform the management of classification of information, the breadth of its scope for classification coupled with the extreme criminal penalties for 'contraventions' of the law were consistently deemed by experts as an unjust infringement on the rights of access to information and freedom of expression.[51]

National security concerns have also been used to justify laws, which legitimise communications interception to a significantly intrusive degree. The Interception of Communications Act of 2007 in Zimbabwe, for instance, is exceptionally broad and essentially allows for opaque oversight of civilian

communications. Further perpetuating this contravention, the government purchased 51% of the information communication services provider, Portnet Software, through Zarnet (which is wholly government-owned) to consolidate control of ICT's in the country.[52]

The Global Principles on National Security and the Right to Information (the Tshwane Principles)[53] serve as a legislative instrument, which seeks to balance the right of access to information with national security concerns particularly as they relate to classification. This is highly relevant within the online space given the ease with which classified data may be broadly disseminated. In many spaces, these principles can serve to counter a historical legacy of secrecy. The British colonial government created the Official Secrets Act, which was a law based on national security that allowed for the classification of documents on the basis of security concerns, and extreme penalties for the release of any such classified information. This law has proved to have a devastating and long-term legacy on the African continent. In South Africa, this law was the basis of the Apartheid governments repressive Protection of Information Act (which up till 2016, still technically existed on the statute books). It exists in Zimbabwe, and was used as the basis for classification law in Botswana, amongst other examples.

There is a legitimate concern for the security of persons in relation to online forms of crime. Increased Internet connectivity, while for many reasons positive, comes with consequent risks, and online crime is one of them. The actual cost from cybercrime to the global economy has been stated as 'more than US$445 billion'.[54] Considering the region in particular:

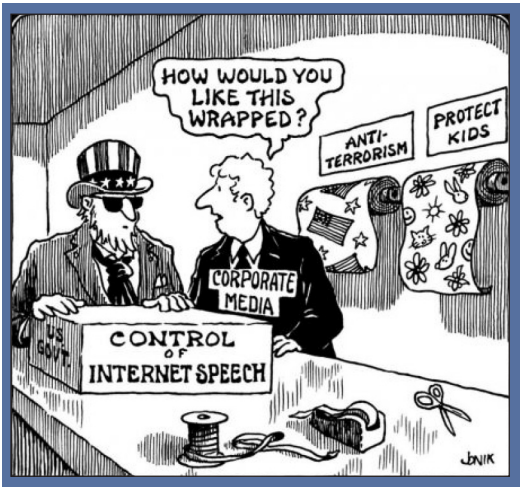
> Africa [is] becoming a cybercrime safe harbour because of increased Internet availability at lower costs, a rapidly growing Internet user base and a dearth of cybercrime laws on the continent. Cybercriminals in Africa are not only using techniques such as the 419 scam or advance fee fraud that originated in Nigeria, but are also deploying more advanced and 'lucrative forms of cybercrime that involve the use of botnets, remote access Trojans, and banking/finance-related malware'.[55]

Not only is personal information easily intercepted, but the anonymity of the Internet makes prosecution a challenge (hampered further by issues of jurisdiction). The ability of the Internet to organise disparate groups could obviously also apply to criminal groups. Yet nevertheless, the adoption of cyber security legislation to combat such crime regionally has been piecemeal

– a result of the growth of ICT's being an accelerated phenomenon, which prevents laws from being comprehensive and consistently developed.[56] This reality inspired the drafting of the African Union Declaration on Cyber Security and Data Protection, 2014. While efforts such as this to provide a regulatory framework for African states is commendable, the obvious first hurdle for the Convention is encouraging countries to ratify. The actual content has not been without criticism, from free speech activists in particular. For instance, the normally broad blanket ban on the processing of personal information without consent is, in this Convention, attenuated with the phrase: 'Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'.[57]

There are also content restrictions for materials that 'insult'; a term that is left unsettlingly vague. While there are other areas of concern, the Declaration is an opportunity for countries to ratify the Convention as a basis for considered and consistent legislating domestically, with reservations noted on the problematic clauses as advised by experts.

As a peculiar space with peculiar vulnerabilities, it is no doubt that regulation will occur. The challenge in the future will be ensuring that sledgehammers are not used for what paintbrushes could deal with. In the area of national security in particular, citizen fear can easily be manipulated by recalcitrant states to renege on freedoms.



This cartoon, by Jonik, was accessed at http://9gag.com/gag/aNnmE6G/how-would-you-like-this-wrapped, sourced http://jonikcartoons.blogspot.co.za/.

Other Rights

More broadly, it is frequently quoted that the Internet is a 'facilitator' of rights. As such a facilitator, there are a variety of substantive rights of influence worth noting, whilst acknowledging this can never be exhaustively done. The interconnection of rights means that determining the influence of the Internet on human rights is a somewhat elaborate exercise, but nevertheless the United Nations Human Rights Council unanimously adopted a resolution proposed by Sweden, that affirmed the need to protect and secure human rights online.[58]

An additional area of intersection worth noting relates to freedom of association. In a modern age, when we consider groups of people organising and assembling, the role of social media and the Internet is clear:

> Using a mix of blogs and social networking sites, the new medium has demonstrated its power to support spontaneous democratic mobilization from below – a concrete and participatory form of democracy.[59]

However, during the 'Arab Spring' it was the Egyptian government's realisation of this power that led to the Internet shutdown described previously. A further interesting recognition of this was in South Africa, where in 2015 the University of Cape Town sought an interdict against protesting students, which included as a party their organising hash tag 'FeesMustFall'.[60] While the Internet may not be the *cause* of organising groups, it is certainly a facilitator. When trying to consider how to protect the freedom of association online, the preservation of anonymity and the permission for encryption become central.[61]

Citizens also have a right to benefit from their intellectual labours. Intellectual property and copyright laws seek to regulate and preserve this right – and the Internet presents several new forms of challenge and opportunity. One such challenge is presented by digital rights management technologies. These are technologies which seek to control copyright, but often give owners significant rights over content purchased by other users. This area of digital censorship will be one to watch moving forward, particularly as citizens of developing countries are more likely to be negatively affected by exaggerated copyright protection of information.[62]

Access

Introduction

We will now turn to the emerging trends on Internet access, which reflect on how and why people may be inhibited from participating in the new Internet jurisdiction. Often a more technical area of regulation, it provides pertinent examples on how structural inequalities in everyday life may be perpetuated, or even exaggerated, online.

Internet Governance

Internet governance refers to the development and application of shared norms and principles by all stakeholders, which seek to shape the evolution and use of the Internet. There are international initiatives that seek to play a role in this, given the manner in which the Internet obliges us to reconsider traditional ideas around 'jurisdiction'. The World Summit on the Information Society and Internet Corporation for Assigned Names and Numbers are examples, but of course there are domestic and regional trends that feed into Internet governance as well. Because of its broad definition, it could consider content regulation, filtering, jurisdiction, naming conventions, etc. It is therefore a sound start to an investigation on trends as a broad catchall before we turn to more specific concerns in relation to access.

In the early days of development, Internet freedom activists envisioned the Internet as a particularly special place, in which the minimum amount of regulatory intervention should be experienced. The idea of 'minimum', however, has become a shifting goalpost as the ubiquity of the Internet has advanced, though concerted international regulation has remained *ad hoc*. This increased focus on the bounds of governance is both as governments try and exert power, but also as we realise that other rights and freedoms need *protection* through intervention for freedom to be a reality.

The Freedom House, 'Freedom on the Net' Report for 2015, notes that freedom on the Internet has been in decline for the fifth year in a row.[63] The methodology for the report included considering interventions into the content sphere and, in so doing, was able to note declines, for example, within Libya that included, "… increase in violence against bloggers, new cases of political censorship, and rising prices for internet and mobile phone services'.[64] Comparatively,

Zambia showed a marked improvement in the reduction in restrictions on its content from previous years.[65] The broad monitoring of Internet freedom is such a necessary concern because, as Lucchi poignantly noted:

> The Internet has become an essential instrument and can now be viewed as a condition necessary for the proper enjoyment of a series of rights, including the rights to access information and to communicate. As a consequence, any regulatory and policy measures that affect the digital-information infrastructure and its content should be consistent with the basic rights and liberties of human beings.[66]

Piecemeal regulation of the Internet is a consequence both of the broader international *ad hoc* regulation, but also a result of the rapid developments in technologies, which lawmakers struggle to keep up with. A regional response has been the multi-stakeholder development of the African Declaration on Internet Rights and Freedoms, which has sought to provide regionally specific principles to guide governance. Perhaps most importantly, it states that the first principle of relevance is that openness:

> The Internet should have an open and distributed architecture, and should continue to be based on open standards and application interfaces and guarantee interoperability so as to enable a common exchange of information and knowledge. Opportunities to share ideas and information on the Internet are integral to promoting freedom of expression, media pluralism and cultural diversity. Open standards support innovation and competition, and a commitment to network neutrality promotes equal and non-discriminatory access to and exchange of information on the Internet.[67]

In many senses, collusion, persecution or agreements between state governments and Internet Service Providers have been examples of a sort of indirect control over the Internet that contradicts such openness.[68] In fact, one of the alleged first incidences of Internet 'censorship' was experienced in 1996 in Zambia, when the government, under threat of criminal prosecution of the relevant Internet Service Provider (Zamnet), forced the removal of a banned edition of the Post Newspaper.[69] However, when a United States based reader posted a version on a United States hosted site, the ban was rendered useless, given the limit of Zambian prosecutorial jurisdiction.

Domestic attempts at governance, which have more directly interfered with freedom, have occurred as well. In 2011, when former President Hosni

Mubarak shut down the Internet and cell phone access in Egypt during the 'Arab Spring' through collusion with three major telecoms companies — Vodafone, Mobinil and Etisalat.[70] This Act was later declared 'unconstitutional', resulting in fines on the basis that the interventions were done without the appropriate attendant court orders.

Perhaps one of the most pertinent concerns for attempts to govern the Internet are that modern concepts are sometimes adequately dealt with within existing frameworks, but in other instances may require innovative thinking. For instance, search engine algorithms – the magical mathematical concoctions that practically govern the way we navigate the Internet – how might they be considered by the law? Guy Berger, of UNESCO, raised this question in 2015:

> …few people know that Facebook uses algorithms to serve us particular feeds of information on 'our' timelines. Likewise with Google, in serving us particular kinds of search results. Perhaps these services suit our needs, and it may be that we have no legitimate claim to such privately created and owned information machines; indeed we can take their offerings or leave them if we do not like the algorithmic secrecy. But in the case of national emergencies at least, we can ask if it not be appropriate for rescue services to be able to have a degree of access to the workings of the algorithms and ability to request tweaks? There may be a need for example to override the automated feed with critical information individuals need to know at key moments.

This highlights another significant issue within the Internet governance sphere that will always be controversial: what is the role of the private sphere in the governance of the Internet space? Without creating corporate accountability in this space, any attempts to preserve certain freedoms in this new 'jurisdiction' may well be worthless.[71]

Infrastructure and Net Neutrality

At its most practical, when we think of access to the Internet, issues around the physical infrastructure of the Internet come to mind. Just because it's a technical issue, does not mean that there are not human rights issues worth reflecting on of importance for the African continent. The law finds a way to infiltrate these areas, and regulation of the telecommunications sector has a significant impact on both the cost of, and access to, the Internet.

State monopoly of infrastructure may have a real impact on people's ability to communicate. This was recognised in the Zimbabwean case of *Retrofit (Private Limited)* vs *Posts and Telecommunications and Another*[72]. In this case, the state refused a license to a company to operate a mobile cellular telephone service. The Supreme Court ruled that such a refusal violated the applicant's freedom of expression, but was also an indication of how state monopolies on infrastructure can affect citizens' rights to communicate. In a poignant exploration of the foundations of the right to freedom of expression, the court held:

> … It assists in the discovery of truth.

The search for truth rationale has been articulated in the famous 'marketplace of ideas' metaphor. This holds that the truth will emerge out of the competition of ideas. In his classic dissent in Abrams v US 250 US 616 (1919) at 630, the redoubtable Justice Holmes said that:

> … when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas – that the best test of truth is the power of thought to get itself accepted in the competition of the market; and that truth is the only ground upon which their wishes safely can be carried out.

This is an interesting judgment, because it suggests that, not only can a monopoly have an influence on cost, but also on the substantive value of free expression.

When we look at a country, such as Ethiopia, monopoly over the ICT sector, coupled with policies limiting growth, have meant prohibitive costs, limits to access (only 0.5% of the population have access to fixed broadband connections) and slow connection speeds.[73] In 2008, research across seventeen African countries concluded:

> The almost uniformly high cost of communications services across the continent continues to inhibit the uptake of services and their usage by consumers.[74]

The way the market is structured clearly impacts this cost. Monopolies, even in the name of universal access, impact the pricing.[75]

We reflect here too on the issue of 'net neutrality'. We can consider this under the category of infrastructure simply because it concerns how data flows through the channels that are available to it. Net neutrality is a concept, which proposes that network owners need to treat all data 'equally'. In other words, network providers should not interfere with the prioritisation of data flowing through the Internet. This is incredibly significant for the African continent, though often spoken about in a United States context given the recent controversy over Federal Communications Commission regulations that received significant citizen pushback.[76] This is because one of the areas in which telecommunications have a vested interest in limiting data is with "… blocking Voice over IP (VoIP) services that may compete with their traditional telephone services".[77] In Africa, VoIP is a service of increasing relevance to African users who, trying to avoid uncompetitive data pricing, rely on VoIP to communicate more cheaply.[78] Artificial interference by telecoms impacts access to this cheaper communication method – and can also be used to interfere with access to a broad range of content.

Digital Migration

'Digital migration' is a catchphrase that has dominated headlines across the world. It involves the international transition from analogue television to digital terrestrial broadcasting, which changes the manner in which signal is distributed to televisions. The transition gives a clearer signal, improved provision of content and choice, a better utilisation of frequencies, as well as user interface benefits. A significant benefit as well for the African content is the 'digital dividend', which refers to the amount of additional radio spectrum created by the move.

The International Telecommunications Union set June 2015 as the 'deadline' for migration, but many African countries have struggled to meet this deadline given funding and infrastructural challenges. Yet, Tanzania has demonstrated some best practice in relation to the process. Not only did it beat the deadline, it completed the challenge in just over two years (comparatively, the United Kingdom took almost two decades).[79]

The human rights implications of digital migration are significant. Migration is an important concern for access, not just for Africa, but globally. If the process

is mismanaged in a national context, large portions of the population will resultantly be left without access to their televisions. This lack of 'access' has implications, both directly on the rights of access, and also in relation to the other substantive rights affected by being disconnected.

One influence on the question of access is the cost of set-top boxes – the device used to read convert digital signals into analogue for televisions that do not yet have a digital function. It was noted, specifically within the Ugandan context that for citizens to afford televisions with digital receivers would merely serve as an additional cost that prohibits access, in a context in which the digital divide sees 25.5% urban Ugandans with televisions compared to 2.6% of rural Ugandans with access.[80] There is the opportunity for states to subsidise the cost of these boxes within their migration policies, but that still has obvious cost implications for the nation as a whole.

There are also lesser thoughts about risks that digital migration may directly contribute to. In South Africa, in a direct acknowledgment of the cost implications for trying to implement a digital migration policy, National Treasury announced Cabinet's approval of increased expenditure for associated projects of around ZAR 1 billion.[81] Problematically though, project spending is easily misallocated or subject to corrupt tender practices, which will be a growing area of concern as expenditure incrementally increases.

Further, in Kenya, during the early days of transition, difficulties abounded.[82] It is not just the physical process that presents challenges, but also how the manner of digitisation may allow for more significant intervention. Because the Kenyan Broadcasting Corporation is potentially going to be the sole distributor, as a centralised model has been decided on to ease costs, some critics have raised concerns about the increased power the broadcaster has to interfere with the distribution of content.[83]

Interestingly too, areas of intellectual property (and their association to various applicable human rights spectrums)[84] may be impacted. This is because digital content is often regulated in a significantly different way to analogue, and contradictions or confusions may consequently occur.[85] That is probably one of the most important flags: will national laws be able to adapt quickly, cohesively and in a considered manner to deal with digital content and broadcasting?

Inequality and the Digital Divide

Substantively underscoring human rights tenets is the idea that, to ensure the full respect of human dignity inherent to each person, people should be treated equally. Kantian philosophy has served as a profound source of inspiration for conceptualising the concept of human dignity, identifying three core components:

1. That every human, by birth, is imbued with dignity;
2. This dignity and worth stems from the fact, that we are rational and moral agents; and
3. Because humans have this worth, there is naturally an obligation of 'beneficence' to one another.[86]

This is important, for instance, the African Union Declaration on Human and Peoples Rights recognises the right to be treated equally by the law[87] – equality between persons requires more than that, bearing both horizontal and vertical elements. What does this mean for the rise of the Internet and technology access on the African continent? It means that one the greatest substantive areas of concern must be to consider the right to equality, in both problem thinking and solution design, politically and practically.

It is this focus on equality (and inequality) that obliges discussion in more detail of the 'digital divide'. This divide refers to the differential access to Internet and telecommunications between persons. It adds an additional axis of inequality for those who have little and is starkly realised on the African continent in a broader context which sees Sub-Saharan Africa as the least developed region of the world, in terms of life expectancy, school enrolment ration, income and under-nourishment.[88] Alongside socio-political impacts, there is an economic impact. One estimate suggests 99.9% of e-commerce will take place only in the developed regions of North America, Europe and Asia Pacific.[89] The digital divide grows as a concern, not just as an additional form of deprivation, but also as this deprivation prevents the attenuation of other disadvantages that access may have assisted with.

Differential access has technical roots. As a 2008 ICT Access Survey summarily noted:

> Broadband access across sub-Saharan Africa is still nascent, but with increased roll out of fixed wireless services such as CDMA and Wimax this is beginning to change. The high cost of computers and the low

> uptake of them by households suggest that limited mobile Internet usage is more likely, though currently far too expensive for generalised use. Only South Africa had any significant uptake of ADSL and mobile HDPSA services…but with ADSL offerings emerging in the dynamic Kenyan and Nigerian markets…
>
> Internet penetration is uneven across the continent, though public access appears to be more pervasive in West and East Africa, most particularly Benin, Burkina Faso, Cameroon, Senegal, Nigeria, Tanzania and Kenya. However, with low home-PC penetration rates across the continent, private access remains very limited, very expensive and way below the critical mass required for it to impact significantly on the economy and society…[I]n the Southern African region the primary point of access to Internet services for many people is at work or school. This is certainly the case for Botswana, Namibia, South Africa and Zambia.
>
> One of the reasons for the high cost of Internet services on the continent is the exceptionally high cost of international bandwidth.[90]

We must, however, understand a 'lack of access' not just being due to physical access to a computer, or a lack of Internet connection, or even merely due to cost, but that issues such as language also have a pertinent role to play. English literacy stands as a significant inhibitor to many on the continent, as the majority of Internet content is still anglicised. These sorts of factors also contribute to the understanding that, while problems of access have technical aspects, structural problems are at the source of the digital divide. This means that policy solutions which focus merely on economic aspects of policy to address technical concerns, fail to adequately improve the divide. In Ghana, for instance, the liberalisation of telecommunications markets at the suggestion of the World Bank and International Monetary Fund, envisioned for improving access, still sees a low level of Internet users, given their income and poverty gap.[91]

There are both international and national dimensions to the digital divide. At the international, the differences between developed and developing countries are marked.[92] However, the national divides are just as pertinent.[93] South Africa is the least connected than any other upper middle-income country, yet the most connected on the African continent.[94] Domestically, only one in three people are Internet users, but two thirds of that number are daily

users.[95] The profile of those users demonstrate too how privilege and access intertwine: 76% of the users live in urban areas and 63% are employed or in education, with 65% educated to at least High School level.[96]

The problem of the divide can be assisted (but not solved) by additional initiatives that also recognise the divide when exploring technology and accountability. For instance, in Liberia,[97] a project funded by the Accountability Lab recognised that, while political information was readily available online, differential access meant that this did not truly equate to 'availability' for all people. The initiative therefore sought to translate the information available simply and clearly through the low-tech solution of a painted daily billboard in a prominent town square.[98]

The divide needs to be addressed because, as noted by former UN Secretary-General Kofi Annan in 1999:

> Three days from now, the world's population will pass the six billion mark. Five out of those six billion live in developing countries. For many of them, the great scientific and technical achievements of our era might as well be taking place on another planet … The capacity to receive, download and share information through electronic networks, the freedom to communicate freely across national boundaries – these must become realities for all people … These people lack many things: jobs, shelter, food, healthcare and drinkable water. Today, being cut off from basic telecommunications services is a hardship almost as acute as these deprivations, and may indeed reduce the chances of finding remedies to them. [99]

Conclusion

The Internet intersects across all aspects of our lives and across all human rights. Thus threats to freedom of expression and access to information online can occur through a variety of legislative and practical interventions. The broad arena of threats is further made difficult by the piecemeal regulation of the Internet, and complicated by the obvious difficulties of jurisdictional space. It is a new frontier – and a new frontier of profound importance for the African continent.

Yet there is not a significant body of work that looks at the Internet (and ICT's) in the realm of human rights in a consistent manner. This may explain some of the erratic and anomalous laws and judgments, from various areas of the continent, which threaten human rights. Further, many of the transgressions are purposefully oppressive, and human rights activists should band together within this new jurisdiction to monitor and act against these transgressions.
The Internet has immense disruptive potential for social justice activists. The Internet is a space for innovation, and there is probably no area more in need of profound innovative thinking than that which seeks to advance human rights. As Eric Schmidt (founder of Google) was famously quoted as saying:

> The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had.[100]

Yet, regulation will only increase. We need to step back and consider how this regulation can be implemented in a consistent manner, and in the advancement of the human rights agenda.

Endnotes

Introduction

1 Silva, A (2013) "Internet Freedom is Not Enough: Towards an Internet based on human rights", Int'l J. on Hum. Rts, 18 SUR (2013) 12-31, at 17.

2 La Rue, F (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, Seventeenth session Agenda item 3, United Nations General Assembly, 16 May 2011 at para 21.

Content

3 For a very interesting and critical discussion on the "Indivisible, Interdependent, and Interrelated" nature of human rights, see Whelan, D (2010) Indivisible Human Rights: A History (USA, Pennsylvania Press).

4 Sconlen & Holderness v Zimbabwe 297/05 (ACHPR), at para 108.

5 La Rue, F et al. (2011), Joint declaration on freedom of expression and the internet (United Nations), available at: https://www.article19.org/resources.php/resource/3313/en/. This quote is also highly relevant to our later discussions on net neutrality.

6 Freedom House (2015) Freedom on the Net: 2015 (Washington DC, Freedom House), at 6.

7 Ibid.

8 Article 19 (2013) The Gambia: New internet law furthers government crackdown on free expression, available at: https://www.article19.org/resources.php/resource/37152/en/the-gambia:--new-internet-law-furthers-government-crackdown-on-free-expression, accessed 01.02.16.

9 Amnesty International (2015) Amnesty International Report 2014/2015: The State of the World's Human Rights (United Kingdom, Amnesty International), at 157.

10 Freedom House (n 6) at 290.

11 There is a rich online resource in this regard available at: http://datajournalismhandbook.org/.

12 See more at https://www.torproject.org/index.html.en.

13 De Vos, P (2015) "Freedom of Hate Speech? No, Thanks", Daily Maverick, available at: http://www.dailymaverick.co.za/opinionista/2015-02-26-freedom-of-hate-speech-no-thanks./#.VdrYzkW1z4Q, accessed 07.09.2015.

14 Buni, C and Chemal, S (2014) "The Unsafety Net: How social media turned against women", The Atlantic, at: http://www.theatlantic.com/technology/archive/2014/10/the-unsafety-net-how-social-media-turned-against-women/381261/, accessed 01.02.2016.

15 Ibid.

16 Ibid.

17 McGonagal, T (2013) "The Council of Europe against online hate speech: Conundrums and challenges", Background paper for Polish Government and Council of Europe conference, The hate factor in political speech – Where do responsibilities lie?, Warsaw, 18-19.9.2013, pp. 4-6, 28-29.

18 Balkin, J (2004) "Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds". Faculty Scholarship Series. Paper 239, available at: http://digitalcommons.law.yale.edu/fss_papers/239.

19 Ibid at 2046.

20 Mendel, T (2013) "Freedom of Information: An Internationally protected Human Right", Comparative Media Law Journal, No. 1 January-June 2003, at 7. Article 19 of the Declaration states: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

21 See for instance section 32 of the Constitution of the Republic of South Africa, 1996; or article 44 of the Constitution of the Republic of Estonia, 1992.

22 Gomes-Lund et al. (Guerrilha do Araguaia) v. Brazil, Inter-American Court of Human Rights (IACrtHR), 24 November 2010.

23 Mendel (n 20). See also article 19 of the International Covenant on Civil and Political Rights and the UN Human Rights Committee General Comment No. 34, adopted in 2011, which states that Article 19(2) of the ICCPR includes the right of access to information held by public bodies.

24 Lucchi, N (2014) "Internet Content Governance and Human Rights" V and. J. Ent. & Tech. L., (17) 809, at 817.

25 These connections were well foreshadowed by the work of the World Information Society, for instance in their 2003 Declaration of Principles available at: http://www.itu.int/net/wsis/docs/geneva/official/dop.html, accessed 01.02.16.

26 Berger, G (2015) Anders Chydenius – Press Freedom 250 years, Opening Remarks at the 250th anniversary year of Nordic "principle of publicity", 4 December 2015,

available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/remarks_berger_250_foi_1.pdf, accessed 01.02.16.

27 Mwsegigwa, P (2015) "Algeria" in C. Estalella, State of Right to Information in Africa: 2015 Report (AFIC, Uganda) at 4.

28 Mutuku, L & Mahihu, C (2014) Open Data in Developing Countries, available at: http://www.opendataresearch.org/sites/default/files/publications/ODDC%20Report%20iHub.pdf (accessed 02.02.16) at 54.

29 Klitgaard, R (1998) "International Cooperation Against Corruption", in Finance & Development March 1998, available at: http://www.imf.org/external/pubs/ft/fandd/1998/03/pdf/klitgaar.pdf, accessed 02.02.16.

30 World Justice Project (2016) Open Government Around the World, available at: http://worldjusticeproject.org/open-government-index/open-government-around-world, accessed 01/02/16.

31 Transparency International (2014) Corruption Perceptions Index: Results 2014, available at: http://www.transparency.org/cpi2014/results, accessed 01.02.16.

32 Yu, H & Robinson, D (2012) "The New Ambiguity of Open Government" 59 UCLA L. Rev. Disc, http://www.uclalawreview.org/the-new-ambiguity-of-"open-government"/, at 178.

33 Ayagre, P & Aidoo-Buameh, J (2014) "Whistleblower reward and systems implementation effects on whistleblowing in organisations" in European Journal of Accounting Auditing and Finance Research, Vol.2, No.1, pp.80-90, at 83, at 83.

34 New York Time Editorial Board (2014) Edward Snowden, Whistleblower, available at: http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?_r=0, accessed at 02.02.16.

35 Whistleblower Act 270 of 2006, at section 23 (Ghana).

36 Ibid at section 24.

37 See for instance Razzano, G (2016), Heroes Under Fire (South Africa: FesMedia), available at: http://www.odac.org.za/images/docs/publications/HeroesUnderFire.pdf, accessed 01.01.16.

38 See further https://afrileaks.org/.

39 Office of the United Nations High Commissioner for Human Rights (2014) The right to privacy in the digital age, A/HRC/27/37 (United Nations), available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf, available 01.01.16.

40 Lucchi (n 24) 831.

41 Electronic Frontier Foundation (2014) American Sues Ethiopian Government for Spyware Infection, available at: https://www.eff.org/press/releases/american-sues-ethiopian-government-spyware-infection, accessed 02.02.16.

42 Electronic Frontier Foundation (2012) Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA, at https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa, accessed 02.02.16.

43 Kaye, D (2015) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council Twenty-ninth session, Agenda item 3, A/HRC/29/32.

44 Telecom Fraud Offence Proclamation 761/2012, sects. 3–10 (Ethiopia).

45 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) ECLI: EU: C: 2014: 317, C-131/12.

46 For a fascinating critique of the growth and death of privacy as a right see: Ferenstein, G (2015) The Birth and Death of Privacy: 3000 years of history told through 46 images, available at: https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e#.c5mto3i4c, accessed 02.02.16.

47 Gwagwa, A & Wilton, A (2014) Protecting the right to privacy in Africa in the digital age (Djibouti, IDRC), available at: https://www.unwantedwitness.or.ug/Protecting-the-right-to-privacy-in-Africa-in-the-digital-age.pdf, accessed 02.02.16, at 4.

48 Mendel, T (2003) 'National Security vs. Openness: An Overview and Status Report on the Johannesburg Principles' in National Security and Open Government: Striking the right balance, Campbell Public Affairs Institute: Syracuse University, New York, p.1-33.

49 Waterfield, B (2008) "EU Plan: The rise and rise of securocrats", Telegraph: online, available at: http://blogs.telegraph.co.uk/news/brunowaterfield/4841723/EU_plan_The_rise_and_rise_of_the_securocrats/, accessed 02.02.16.

50 At the time of writing, the President had still not yet signed this Bill, though passed by the national assembly, into law.

51 See for instance De Vos, P (2013) New Improved Secrecy Bill: still bad, still unconstitutional, available at: http://constitutionallyspeaking.co.za/new-improved-secrecy-bill-still-bad-still-unconstitutional/, accessed 02.02.16.

52 Ndebele, H (2015) Portnet acquisition: Govt tightens grip on internet communication, available at: http://www.theindependent.co.zw/2015/09/11/portnet-acquisition-govt-tightens-grip-on-internet-communication/, accessed 02.02.16.

53 Download at http://www.opensocietyfoundations.org/publications/global-principles-nationalsecurity-and-freedom-information-tshwane-principles.

54 Tamarkin, E (2015) "The AU's cybercrime response: A positive start, but substantial challenges ahead", in ISS Policy Brief 73, January 2015.

55 Ibid at 3.

56 Gasser, U (2006) 'Regulating Search Engines: Taking stock and looking ahead' in Yale Journal of Law and Technology, 8:1, 202-234.

57 African Union Declaration on Cyber Security and Data Protection EX.CL/846 (XXV) at article 14.2.i.

58 The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/26/13.

59 Lucchi (n 24) 831.

60 University of Cape Town v Rhodes Must Fall and Others Case No. 20182/2015 WCD, unreported.

61 Deb, B & Pessoa, J (2014) IGF 2015: The right to protest online, available at: https://www.apc.org/en/blog/igf-2015-right-protest-online, accessed 02.02.16.

62 Nicholson, D (2009) "Digital Rights Management and Access to Information: a developing country's perspective" Library and Information Science Research Electronic Journal, 19: 1, at 13.

Access

63 Freedom House (n 6).

64 Ibid at 2.

65 Ibid at 3.

66 Lucchi (n 24) 851.

67 African Declaration on Internet Rights and Freedoms (2015), available at: http://africaninternetrights.org/updates/2015/11/article-450/articles, accessed 02.02.16

68 Lucchi (n 25) 819.

69 Burnheim, S (undated) Censorship and Control: obstacles to growth, available at: https://www.article19.org/data/files/pdfs/publications/africa-internet.pdf, accessed 02.02.16.

70 MacKinnon, R et al. (2015) Fostering freedom online: the role of Internet intermediaries (France: UNESCO) at 94.

71 For a fuller consideration of the rights, see Silva (n 1).

72 Retrofit (Private Limited) v Posts and Telecommunications and Another 1995 (2) ZLR 199 (S) 211-213.

73 Freedom House (n 6).

74 Gillwald, A & Stork, C (2008) ICT Access and Usage in Africa, available at: http://www.researchictafrica.net/publications/Towards_Evidence-based_ICT_Policy_and_Regulation_-_Volume_1/RIA%20Policy%20Paper%20Vol%201%20Paper%202%20-%20ICT%20Access%20and%20Usage%20in%20Africa%202008.pdf, accessed 02/02/16 at 31.

75 Ibid at 2.

76 Freedom House (n 6) at 12.

77 Ibid.

78 Research ICT Africa (2014) Shift from just voice services: African markets gearing for internet, available at: http://www.researchictafrica.net/polbrf/Research_ICT_Africa_Policy_Briefs/2014_Policy_Brief_1_Shift_from_just-voice_-_African_markets_gearing_for_internet.pdf

79 http://www.ippmedia.com/frontend/index.php?l=87130, accessed 01/02/16.

80 Mubangizi, M (2015) Digital migration will widen gap between information haves and have-nots, available at: http://www.newvision.co.ug/news/670128-digital-migration-will-widen-gap-between-information-haves-and-have-nots.html, accessed 02.02.16.

81 TechCentral (2011) South Africa will give more money for digital TV, available at: http://www.balancingact-africa.com/news/en/issue-no-534-0/web-and-mobile-data/south-africa-will-gi/en, accessed 02.02.16.

82 Mwitit, L (2015) Lies, damn lies, and statistics: 15 big facts about the digital migration war in Africa, available at: http://mgafrica.com/article/2015-02-24-by-the-numbers-15-bighugestaggering-facts-about-digital-migration-in-africa, accessed 02.02.16.

83 Burgess, J (2009) Throwing the Switch: Challenges in the Conversion to Digital Broadcasting (Washington DC: CIMA) at 21.

84 See for instance World Intellectual Property Organisation (1998) Intellectual Property and Human Rights (Geneva: WIPO), available at: http://www.wipo.int/edocs/pubdocs/en/intproperty/762/wipo_pub_762.pdf, accessed 01.02.16.

85 Muheebwa, H (2015) Digital Migration Brings New Intellectual Property Challenges, available at: http://www.ip-watch.org/2015/06/16/digital-migration-brings-new-intellectual- property-challenges/, accessed 02.02.16.

86 Rachels, J (1986) "Kantian Theory: The Idea of Human Dignity", available at: http://public.callutheran.edu/~chenxi/phil345_022.pdf, accessed 02.02.16.

87 While contained in Article 3, there are several notable mentions of equality of persons through out the text.

88 Fuchs, C & Horak, E (2008) "Africa and the digital divide" Telematics and Informatics 25 (2008) 99–116, at 99.

89 Dholakia, N & Kshetri, N (2005) Digital Divide to Digital Dividend, available at: SSRN: http://ssrn.com/abstract=847186, accessed 02.02.16, at 1.

90 Gillwald & Stork (n 74) at 33.

91 Fuchs & Horak (n 88) at 113.

92 Dholakia & Kshetri (n 89).

93 Consider even the impact in countries such as the United States of America that, while "developed", still have significantly differential access between communities that impacts broader human rights, Burrington, I (2015) Where the Clouds Rise from the Sea, available at: http://www.theatlantic.com/technology/archive/2015/11/where-the-cloud-rises-from-the-sea/415236/, accessed 02.02.16.

94 De Lanerolle, I (2012) The New Wave: Who connects to the internet, how they connect and what they do when they connect (South Africa: Wits Journalism, University of Witwatersrand) at 7.

95 Ibid at 6.

96 Ibid at 8.

97 Urdaneta, J (2013) Liberia: A Journalist, a Blackboard, Some Chalk and Open Government, available at: https://www.globalintegrity.org/2013/06/liberia-low-tech-billboards/, accessed 02.02.16.

98 Ibid.

99 Quoted in Fuchs & Horak (n 88) at 99.

Conclusion

100 Singer, P & Friedman, A (2015) Cybersecurity and Cyberwar: What everyone needs to know (New York: Oxford University Press) at 27.

FRIEDRICH EBERT STIFTUNG

fesmedia Africa *series*