The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain

by Alex Comninos

Intermediary Liability in Africa Research Papers, No. 1

Independent research commissioned by the Association for Progressive Communications and supported by Google and the Open Society Foundation

October 2012

Table of Contents

This paper is part of a research project conducted on intermediary liability in Nigeria, Kenya, South Africa and Uganda. The paper draws on the independent research conducted by in-country researchers. The research includes five reports, as well as blog posts. The entire research is available at http://ila.apc.org.

Introduction

Intermediary liability refers to when internet intermediaries involved in the transmission processing or storage of electronic data across on the internet are held liable for unlawful content transmitted or stored on their networks. According to the OECD "internet intermediaries bring together or facilitate transactions between third parties on the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet based services to third parties."[1] It is inevitable due to the openness of the internet that "some users will post content or engage in activity that is unlawful or otherwise offensive."[2] Sometimes intermediaries may find themselves legally liable for content on their networks created by third parties, including content which they did not even know was on their networks.

It is easier to identify an intermediary than a user, and thus easier to bring them before a court for a criminal or civil offence. Intermediaries also have bigger pockets than the average internet user and can sued in court for damages more easily, and for more money. Intermediaries can be quite vulnerable to governments and corporations. Many governments seeking to use intermediaries to control certain content, also have control over the granting of telecommunications licenses.

Depending on relevant national law, liability for online content of third parties "can arise in a number of situations, both legitimate and politicised, including for defamation, obscenity, invasion of privacy, intellectual property infringement, or because the content is critical of the government."[3]

For governments, intermediaries "represents a potential point of control over content or unlawful behaviour." Private actors may "also threaten expression and innovation online if they can bring civil lawsuits against the intermediaries that host or disseminate expression that the private parties seek to suppress. "[4] Intermediary liability has been argued to be an increasing trend globally in which responsibilities of law enforcement, as well as of copyright enforcement are transferred to intermediaries. Internet intermediaries are increasingly used to "police and enforce the law on the internet and even to mete out punishments."[5]

This report forms part of a four-country study that investigates the legislative, legal, regulatory, political and economic frameworks that govern the liability of internet intermediaries in Kenya, Nigeria, South Africa and Uganda. The study provides an overview of the current situation concerning intermediary liability in these countries and how it has changed in recent years. It explores current and past debates on intermediary liability, situations in which intermediaries may be liable for unlawful content posted or transmitted by third parties, and whether there are any protections for internet intermediaries in the form of limitations on liability. This report provides an overview of the concepts of internet intermediaries and intermediary liability. It then examines the human rights effects of intermediary liability, describes limitations on liability in the US and the EU, and argues for the need for protection for internet intermediaries. Issues relating to intermediary liability in Nigeria, Kenya, South Africa and Uganda are then explored. Finally important conclusions from the research are summaries, and a set of recommendations for all stakeholders affected by intermediary liability is

1 OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives (OECD, 2011) 21 http://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives_9789264115644-en

2 Center for Democracy and Technology, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation,* (Center for Democracy and Technology, April 2010) p1, https://www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation.

3 Ibid.

4 Ibid.

5 Joe McNamee, "Internet intermediaries – The new cyberpolice?" in *GISWatch 2011 – Internet Rights and Globalisation,* ed Alan Finlay, (Johannesburg: APC & HIVOS, 2011), 27.

provided.

Although addressed explicitly in South African legislation since 2002,[6] and in Ugandan legislation since 2011,[7] intermediary liability, termed as such, is a relatively new debate in Kenya, Nigeria and Uganda. While there is quite a substantial amount of literature on intermediary liability in Europe[8] the United States of America (USA) and other countries. There is little existing literature comparing intermediary liability in African countries, and there are few developed African case studies.[9] Considering that intermediary liability research is driven by policy and legal debates, and that policy discussion expressed as "intermediary liability" has been absent in the countries in the study until recently, this situation not surprising. Thus this study is an exploratory study; it does not provide an exhaustive overview of intermediary liability in all the respective countries, it rather investigates important issues and themes framing the discussion in contemporary debate, and points towards strategic points for further research, advocacy and capacity building.

Conceptualisation

Internet intermediaries comprise the pipes through which internet content is transmitted and the storage spaces in which it is stored. Intermediaries[10] are essential to the functioning of the internet. They act as intermediaries between two or more nodes on a network: as mere conduits for the transmission (sending or receiving) of information/data, as online storage spaces for online data, as platforms for storage and sharing of user generated content (UGC), or as platforms that provides links to other internet content. Intermediaries perform a passive and automatic role in the storage and transmission of electronic data, information or content – they are not actively involved in, and do not actively initiate the transmission or storage of data; this is done automatic manner and as a component of a service that is provided by the intermediary.

An internet service provider (ISP), that provides services like email or FTP is an intermediary. So is an internet access provider (IAP), which provides access to the internet.[11] When using ISPs and IAPs users simply request a web page or a file, or send an email, and the data is transmitted by an intermediary (most often through a number of intermediaries) to its location. A network operator is also an intermediary; its business is the transmission of data between points on the network as well as other networks. Using the example of a mobile network operator; a user request information from a website or online service data is transmitted to the mobile device without active intervention or participation of the network operator.

Similarly internet cafes, or cybercafes can also be considered intermediaries, as they offer other users access to the internet A web host, or web hosting company, which stores web sites, or data or information on the internet for its users, is also an intermediary. The information on its servers, is uploaded and downloaded by

6 By Chapter XI of the Electronic Communications and Transactions Act (Act 25 of 2002), http://www.internet.org.za/ect_act.html

7 Electronic Transactions Act (8 of 2011), http://ict.go.ug/index.php?option=com_docman&task=doc_details&gid=59&Itemid=61

8 The European Commission has commissioned a regional study on intermediary liablity, Verbiest, Spinner, Riccio, and Van der Perre, Study of the Liability of Internet Intermediaries, (European Commission, 12 November 2007), http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

9 While there is some vibrant policy discussion and some academic law papers from South Africa; the most comprehensive studies are Masters' theses, this reflects the current dearth of the literature. See N.D. O'Brien, The Liability of Internet Service Providers for Unlawful Content Posted by Third Parties, Masters Thesis, Faculty of Law at the Nelson Mandela Metropolitan University, January 2010, http://dspace.nmmu.ac.za:8080/jspui/bitstream/10948/1149/1/NDOBRIEN.pdf and Olumuyiwa Oluwole Popoola, Statutory Limitation of Liability of Internet Service Providers in Decentralized Peer to Peer File Sharing, University of South Africa, February 2012, http://uir.unisa.ac.za/bitstream/handle/10500/5618/thesis_popoola_o.pdf?sequence=1 .

10 Hereafter, the terms "Internet intermediaries" and "intermediaries" are used interchangeably.

11 In common usage IAPs are called ISPs, as most ISPs offer services (like email and hosting in addition to access).

users by means of automated processes without direct intervention by the hosting company.

Social networking platforms like Facebook, LinkedIn, Orkut and Pinterest are also intermediaries. They play an automated role in the storage of and sharing of content between different users of the platforms. UGC platforms like the blogging site Tumblr, or the microblogging site Twitter are intermediaries. YouTube, image picture sharing sites like FlickR , and blogging platforms like Wordpress.com, provide platforms for users to upload, share and access content. Search engines also perform the role of internet intermediaries – providing links to websites that are searched for and retrieved automatically with computer algorithms. Content aggregators which automatically compile content from different online sources can also be intermediaries.

If an online entity performs a service that is automatic, and in which they are not actively involved in creating and selecting data, then they may function as an intermediary. Thus a news site, or even a blog may under certain conditions be an intermediary. Although they may publish their own content, if there is a comments section, forum, or some kind of hosted discussion, then the site acts as an intermediary for an automatically facilitated hosted discussion. A blog or news site that does not have comments, discussion, or mechanisms hosting UGC, is not an intermediary. Sites are not intermediaries for content they have actively commissioned or created.[12]

Internet intermediaries

The following could be considered as intermediaries, this list is not exhaustive in listing all possible intermediaries.

- **Network operators** – mobile network operators (e.g. MTN, Safaricom), metropolitan or countrywide network operators, internet exchanges.
- **Network infrastructure providers** that create and maintain networks for network operators, e.g. Cisco, Huawei, Ericsson, Dark Fibre Africa.
- **Internet access providers** – companies that provide access to the internet like Comcast (US), MWeb (South Africa), Kenya (e.g. AccessKenya), also at the smaller scale, internet cafes, cybercafes and Wi-Fi hotspot providers.
- **Internet service providers** – companies that provide internet services like for example email providers. Many IAPs, as well as network operators are also often ISPs and the term is often used interchangeably.
- **Hosting providers** – provide online hosting and storage services.
- **Social Networks** – e.g. Facebook, Twitter, LinkedIn, Orkut, Google + and UGC platforms (blogging platforms, microblogging platforms, video sharing sites, picture sharing sites).
- **Search engines** (and aggregators (e.g. Slashdot or Ushahidi installations).
- **Internet cafes / Cybercafes**
- **Comments sections on blogs or websites**

12 For example a news site is not an intermediary for transmission of content that it has paid for or commissioned for publication on the site, a blog is not an intermediary for content posted by the blog owners, in this case the blog or news site is a publisher.

In performing these roles, intermediaries cannot reasonably be expected to be aware of all the content transmitted, stored or referenced on their networks, which is constantly changing and at an automatic and rapid pace. It is thus argued by many that intermediaries should not be held liable for content on their networks created by third parties.

When does intermediary liability occur?

Intermediary liability occurs "where governments or private litigants can hold technological intermediaries such as ISPs and websites liable for unlawful or harmful content created by users of those services."[13] Intermediary liability can thus occur in a vast array of circumstances, around a multitude of issues including: copy right infringements, digital piracy, trademark disputes, network management, spamming and phishing, "cybercrime", defamation, hate speech, child pornography, "illegal content", offensive but legal content, censorship, broadcasting and telecommunications laws and regulations, and privacy protection.[14]

Often intermediary liability can also occur in the context of laws that have not adequately taken account of the the internet; especially the role of intermediaries. This is the case in Kenya and Nigeria. In these cases, understanding where intermediaries are liable, and where intermediaries are not liable, would entail a comprehensive review of all relevant legislation, criminal law, civil law and common law . Here intermediary liability is generally assessed on a case-by case basis, by reviewing legislation, and by looking at legal precedents.

Intermediary liability can also occur as a result of a conscious effort of governments and other actors to control certain aspects on the internet by holding intermediaries responsible for users. It can be a government or corporate (or combined) strategy for controlling illegal, unlawful, or undesirable content on the internet. This is a strategy adopted by the Chinese government to control aspects of the internet there.[15] In these cases intermediary liability is determined by investigating specific laws that mandate intermediaries to be liable in certain circumstances. There is little evidence to point towards intermediary liability currently being used as an effective cohesive strategy by governments to censor the internet in any of the countries in the study. However, this is always a risk in any society, especially where there is no legislated protection for intermediaries to mitigate for this (like for example in Kenya and Nigeria).

In many countries, there are legislated limitations on liability for intermediaries, often termed "safe harbour". This protection is provided under certain conditions; usually that intermediaries do not actively initiate or consciously modify the transmission, are unaware of unlawful content on their networks, and that they conform with certain laws and practices – like for example responding to take-down requests. In cases where there are limitations on liability, liability can only occur when intermediaries are not protected under existing legislation. This is the case under the South African Electronic Communications and Transactions (ECT) Act (25 of 2002)[16], and the Ugandan Electronic Transactions (ET) Act (8 of 2011).[17]

13 Center for Democracy and Technology, op cit.
14 La Quadrature Du Net Wiki, "Intermediary Liability". http://www.laquadrature.net/wiki/Intermediary_Liability accessed 29 September 2012.
15 Rebecca MacKinnon, "Are China's demands for self-discipline spreading to the West?" (McClatchy, 18 January 2010), http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html. See also: Qian Tao, "The knowledge standard for intermediary liability in China", *International Journal of Law and Information Technology 20(1),* 1-18.
16 http://www.internet.org.za/ect_act.html
17 http://ict.go.ug/index.php?option=com_docman&task=doc_details&gid=59&Itemid=61

Assessing intermediary liability

The human rights consequences of intermediary liability

When intermediaries are exposed to risk for criminal or civil liability for content on their networks, they are incentivised to control or police this content. Globally internet intermediaries are increasingly used to "police and enforce the law on the internet."[18] Intermediary liability can be argued to be a set of strategies for dealing with certain real problems of unlawful content on the internet – for example to curb and control child pornography, hate speech or piracy of copyrighted material. Some of these strategies may however be unfair on intermediaries who did not create the content, where not actively involved in storing, transmitting or referencing it, are unaware of the content. Furthermore, such strategies can also have negative consequences on the functioning and usefulness of the internet.

The most obvious negative consequences are economic. If intermediaries are liable for content transmitted over their networks, then the expense and risk of building and maintaining these networks increases. If network operators were held liable for all criminal acts conducted over their networks, if ISPs were held liable for all unlawful content sent over emails, if hosting providers were liable for all content on their networks, and there were no limitations on this liability, then e-commerce and the information society would grind to a halt.

If user-generated content platforms and social networks are too scared to provide these platforms out of fear of liability, then these services would not be offered, resulting in adverse effects on freedom of speech and freedom of association. When policing roles are transferred to intermediaries this can also have chilling effects. If intermediaries, rather than the courts become responsible for determining what content is lawful and what content is not, this may undermine the right to a fair trial or due process, it can also cause intermediaries to be overzealous in policing content, so as to avoid liability. Intermediary liability may thus "create borders in the online world, undermining the very openness that gives the internet its value for democracy, and indeed, or the economy."[19]

At the extreme end of the potential negative consequences is that governments could use intermediary liability as a means of censorship. For a government seeking to control the internet in a way that undermines human rights, outsourcing control to third parties by mechanisms of intermediary liability can look better than, as well as be more efficient than technical mechanisms such as a web filter would, as Evgeny Morozov has pointed out:

> "One way for governments to avoid direct blame for exercising more Internet control is to delegate the task to intermediaries. At a minimum, this will involve making Internet companies that offer social-networking sites, blogging platforms, or search engines take on a larger self-policing role by holding them accountable that their users post or (in the case of search engines) index and make available.
>
> Being able to force companies to police the Web according to state-dictated guidelines is a dream come true for any government. The companies must bear all the costs, do all the dirty work, and absorb the user's ire. Companies are also more likely to catch unruly content, as they are more decentralized and know their own online communities better than the state's censors."[20]

18 Joe McNamee, "Internet intermediaries – The new cyberpolice?" op cit.
19 Ibid.
20 Evgeny Morozov, "Whither Internet Control?" in *Liberation Technology: Social Media and the Struggle for Democracy*, ed. Larry Diamond and Marc F. Plattner, (Baltimore: Johns Hopkins University Press, 2012).

The need for limitations on liability

According to the Center for Democracy and Technology, "the history of the Internet to date shows that providing broad protections for intermediaries against liability is vital to the future of the Internet."[21] Every society needs limitations on intermediary liability in order for an information economy and information society to function effectively. Thus "protecting intermediaries from liability for the actions of third parties expands the space for online expression, encourages innovation in the development of new services, and creates more opportunities for local content, thereby supporting development of the information society." [22]

During the 1990s – first decade of the popular spread of the internet – it was realised that limitations on the liability of internet intermediaries needed to be legislated for in order to ensure the effective functioning of the internet. Thus many countries have introduced limitations of liability for internet intermediaries.

Box 2: Limitations on liability in the US and E Commerce Directive

The United States of America

Section 230 of the United State's Communications Decency Act of 1996 (referred to as CDA 230) was the first act providing for limited liability of internet intermediaries in the USA.[23] Section 230 provided that internet intermediaries[24] would not be considered publishers, and would thus not be held liable for the content created by third party users of their services.[25] This protection from liability entails protection from most laws broken by the third parties online, except for copyright legislation which is covered by the Digital Millennium Copyright Act.[26]

There are also provisions for the limitation of liability of internet intermediaries for copyright infringements in what are referred to as the "safe harbour" clauses of the The Digital Millennium Copyright Act[27] (in America. The DMCA offers protection from liability for internet intermediaries for copyright infringing content stored and transmitted through their networks under certain conditions. To qualify for this protection, internet intermediaries must: "have no knowledge of, or financial benefit from, infringing activity on its network, have a copyright policy and provide proper notification of that policy to its subscribers, list an agent to deal with copyright complaints."[28] Intermediaries also need to respond to take-down requests and take down copyright

21 Center for Democracy and Technology, Op cit, p2
22 Center for Democacy and Technology, op cit, p1.
23 The CDA attempted to regulate indencency, obscenity and pornography on the internet. The CDA which is in itself an Amendment to the Telecommunications Act. CD 230 is Section 230 of Title 47 of the 47 US Criminal Code, the Text can be seen at "USC § 230 - Protection for private blocking and screening of offensive material" http://www.law.cornell.edu/uscode/text/47/230
24 Defined as "providers" of "an interactive computer service".
25 CDA 230 states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."
26 CDA 230 also states, "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." CDA 230 however does not apply to federal criminal law, intellectual property law, and electronic communications privacy law. See also Electronic Frontier Foundation, Section 230 Protections, (*Electronic Frontier Foundation – Legal Guide for Bloffers,* n.d.) https://www.eff.org/issues/bloggers/legal/liability/230.
27 The Digital Millenium Copyright Act was introduced in 1998 and amends sections 5, 17, 28 and 35 of the United States Code.
28 As summarised at DMCA Safe Harbour (Chilling Effects Clearing House, n.d.), http://www.chillingeffects.org/dmca512/

infringing content in order to keep their protection from liability.

Limitations on liability under the EU E-commerce directive

Under the European Union (EU) E-commerce directive, internet intermediaries[29] are afforded protection from intermediary liability for being a mere conduit for information, for caching information, or for hosting information.[30] Provided that these activities are "of a mere technical, automatic and passive nature" and the intermediary "has neither knowledge of nor control over the information which is transmitted or stored. "[31] In the case of being a mere conduit, or of caching, in order to be protected from liability; the intermediary must not modify transmitted information,[32] and not collaborate with recipients of its services in order to undertake illegal activity.[33] Protection from liability for hosting[34] is conditional on the service provider having been unaware of content on its networks, and once becoming aware of illegal activity on its network, acting expediously to remove it.[35]

Intermediary liability in Nigeria, Kenya, South Africa and Uganda.

Issues relating to intermediary liability vary among the countries in the study but there are many common issues among the countries including the limitations on liability, the role of intermediaries with regards to terrorism and violence, hate speech, cybercrime, copyright infringement, digital piracy, and obligations to assist with lawful interception of communications.

Other than in South Africa policy debates around intermediary liability are relatively new. Limitations on liability were legislated in South Africa in the Electronic Communications and Transaction Act (25 of 2002)[36], almost five years before they were first contemplated in Kenya[37] and almost ten years before they were legislated in Uganda[38]. This is perhaps due to the relatively higher internet penetration in South Africa in the 1990s and 2000s – it had one of the highest rates of internet penetration in Africa and ranked higher than other countries with similar levels of economic development[39]. The absence of mention of intermediary liability in legislation in Kenya, Nigeria and Uganda is perhaps explained by the lower levels of internet access in these countries in the 1990s and 2000s. Now other African countries have overtaken South Africa, which is reported by some studies to have lower levels of internet penetration than Nigeria, Kenya and Uganda.[40] As all countries

29 Termed "information society services".
30 This does not include liability for the protection of individuals with regard to the processing of personal data which "is solely governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (2) and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (3)"
31 Directive 2000/31/EC of the European Parliament and the Council, of June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Article 42. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0001:EN:PDF
32 Except in a technical and automatic manner that does not alter the integrity of the data
33 Directive 2000/31/EC, Op cit, 43, 44.
34 Termed "storing information".
35 Directive 2000/31/EC, Op cit, 46.
36 http://www.internet.org.za/ect_act.html
37 Safe harbour like provisions for liabilities were proposed in the Now Defunct Electronic Transactions Bill of 2007.
38 In the Electronic Transactions Act of 20011, op cit.
39 "South Africa" in Freedom House, *Freedom on the Net 2011, http://www.freedomhouse.org/report/freedom-net/2012/south-africa*)
40 One study reports South African internet penetration at 17%, "it lags significantly behind the biggest Internet user bases of Africa." Nigeria has 29% penetration , Egypt has 26%, Morocco has 49% and Kenya has 25% (Arthur Goldstuck, *Internet Matters in South Africa,* Johannesburg: Word Wide Works, 2012, http://www.internetmatters.co.za/report/ZA_Internet_Matters.pdf). Another study says that in South Africa 48% of people have "ever used the internet" this is compared to 57% in Senegal, 52% for Nigeria and 49% in Ghana, Kenya

have in recent years experienced increased internet access, increased bandwidth and increased access through mobile phones, intermediary liability has emerged in legislative and policy debates.

Nonetheless issues concerning intermediary liability are neither new nor have they arisen out of a vacuum they have been discussed earlier in issue-based contexts using different terminology. In Nigeria the role of cybercafes with regards to cybercrime was discussed in the mid-2000s. As mobile internet access has increased and relative rates of access from cybercafes have decreased the discussion has now moved center around mobile phone operators. In Kenya, after the election violence following the 2007 elections, an ongoing debate about the role of communications intermediaries with regards to hate speech along with their role in peacebuilding began. The debate initially focused on the role of mobile operators and particularly focused on SMS/text messages. The debate continues as Kenya streamlines the writ and interpretation of its legal system to accord with its new constitution. Debate around the role of intermediaries in hate speech and in political messaging has regained momentum as the Kenyan General election approaches on the 4th of March 2013.

Issues

The following issues that are common to two or more countries have arisen from the study.

Protection for intermediaries

In all countries in the study, excluding South Africa there is a significant degree of legislative and regulatory uncertainty with regards to issues around intermediary liability. Regarding limitations on liability for internet intermediaries, or "safe harbour"; only in South Africa and Uganda are there clear pieces of legislation limiting the liability of certain intermediaries for unlawful content under certain circumstances. In Chapter XI of the ECT Act provides internet service providers with protection from liability: service providers are not liable for hosting, being a mere conduit or caching, provided that they conduct their operations in a specific manner, are a member of a recognised industry representative body, and adhere to its code of conduct, and respond to take down notices. The legislation has existed since 2002 but only recently has it come into effect when the minister recognised the Internet Service Providers Association (ISPA) as an industry representative body in 2009. Therefore only the 160 current members of ISPA are provided with limitations on liability. Many cybercafes, individual blog owners, news sites, and other intermediaries that are not members of the ISPA are not afforded the limitations on liability afforded by Chapter XI of the ECT Act.

In Uganda under Section 29 of the Electronic Transactions Act (2011) a a service provider is not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access. This is provided that the intermediary is not directly involved in the making, publication, dissemination or distribution of the material or a statement made in the material; or the infringement of any rights subsisting in or in relation to the material. Section 30 states that service providers are not liable for infringement for referring or linking to a "data message or infringing activity" if the service provider, is unaware of the infringement, does not receive financial benefit from the infringement, and "removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of

and Uganda (Basis Research, Insights Africa, 2012 http://www.insightsafrica.com). According to ITU data from 2010, the "countries above South Africa in terms of internet users per 100 inhabitants are in descending order are: Morocco, Seychelles, Tunisia, Cape Verde, Nigeria, Mauritius, Egypt, Kenya, Sao Tomé and Principe, Libya, Rwanda, and Uganda" ("South Africa" in Freedom House, *Freedom on the Net 2012, http://www.freedomhouse.org/report/freedom-net/2012/south-africa*).

the user."

In Nigeria and Kenya there are no pieces of legislation affording explicit protection for intermediaries. In Nigeria the copyright bill, which is currently under discussion may limit liability for intermediaries for copyrights content, should they be unaware of this content, as well as according to a number of other conditions. In Kenya the now defunct Electronic Transactions Bill of 2007, borrowing extensively from the EU Commerce Directive would have provided limitation on criminal and civil liability for third parties, where they acted as mere conduits, in caching processes, and when used as information location tools. It also had a license and take down procedure, and provided immunity from liability for any actions taken once notified of the infringing activity. It is suggested in the report that this bill may need to be revisited in efforts to ensure that legislation provides for safe harbour for intermediaries.

Hate speech

Hate speech is an important area possibly affecting the liability of intermediaries in all countries. Nigeria, South Africa, Uganda and Kenya all have histories that include violent political conflicts in which hate speech, based on discrimination or ethnicity over mass media and/or ICTs have at some point played a role.

In South Africa, knowingly distributing films that advocate hatred based on race or ethnicity, gender or religion and constitutes and incitement to cause harm is an offence under Section 29 (1-2) of the Film and Publications Act (65 of 1996)[41] punishable by a fine or no more than five years of imprisonment. ISPs can thus be liable if they knowingly distribute hate speech (subject to limitations on liability in the ECT Act). The South Africa Promotion of Equality and Prevention of Unfair Discrimination Act (Act 4 of 2000)[42] makes it a crime to publish speech that could demonstrate a clear intention to be hurtful, harmful, incite harm or promote or propagate hatred. It is also an offence to broadcast or distribute content that amounts clearly intends to unfairly discriminate against any person.[43]

In Kenya the new constitution states that publishers can be held liable for publishing hate speech. Whether this clause in the constitution exposes intermediaries to liability has not been tested yet in courts. Online publishers and media groups are greatly aware of the problem of hate speech, and have made efforts at attempting to control it. For the Nation Media has issues guidelines on blogging and moderating comments.

In September 2012 the Communications Commission of Kenya released "Guidelines for the Prevention of Transmission of Undesirable Bulk Political Content Messages via Electronic Communications Networks". The Guidelines which apply to Mobile Network Operators (MNOs) and Content Service Providers (CSPs) which provide content or content services.[44] They regulate the sending of "political messages" defined as "the transmission of political content by Political Parties and other individuals to the general public by SMS or MMS[45] or any other similar medium that is capable of transmitting bulk."[46] Political messages are not to contain "inciting, threatening, abusive, misleading, confusing, obscene or profane language" or "inciting,

41 http://www.info.gov.za/view/DownloadFileAction?id=70901
42 http://www.info.gov.za/view/DownloadFileAction?id=68207
43 Section 10 and 12.
44 Under Kenya's Universal Licensing regime, "Licensees under this category shall provide contents services material, information services and data processing services." "Market Structure" Kenyan Communications Commission/ http://www.cck.go.ke/licensing/telecoms/market.html
45 Multi Media Message.
46 Communications Commission of Kenya, Guidelines for the Prevention of Transmission of Undesireable Bulk Political Content Messages via Electronic Communications Networks. September 2012. http://www.cck.go.ke/regulations/downloads/Guidelines_for_the_prevention_of_transmission_of_undesirable_bulk_political_content_via_sms.pdf Section 2.1.6

threatening or discriminatory language that may or is intended to expose an individual or group of individuals to violence, hatred, hostility, discrimination or ridicule based on the basis of ethnicity, tribe, race, colour, religion, gender, disability or otherwise." Political messages must also not contain "attacks on individual persons, their families, their ethnic background, race, religion or their associations."[47]

Political messages are only to be delivered by licensed Content Service Providers (CSPs)[48] with inter-operability agreements with mobile operators (MNOs). " MNOs are exempt liability for bulk content sent by third parties but CSPs are required to indemnify themselves (presumably through contractual agreements with the third parties), although it is not specified how. [49] Whilst MNOs are exempt from legal liability, they are presented with responsibility of approving political messages. CSPs need to send an application to an MNO, before sending a bulk political message.[50] MNOs are effectively given the responsibility determining whether political messages approve or conform to the guidelines, and must come to a decision within 18 hours.[51] If the MNO is unable to reach a decision, they may refer the matter to the National Cohesion and Integration Commission.[52]

While many CSPs are not internet intermediaries because they sell content, and are actively involved in selecting the content, many others listed as CSPs perform intermediary functions and could be considered intermediaries.[53] The guidelines would impose possibly liability on CSPs for bulk messages sent by third parties. They would also impose liabilities on internet intermediaries to make censorship decisions, as well as onerous administrative costs. Imposing responsibility to moderate content on private corporations (MNOs) rather than industry bodies may have negative effects on transparency, or freedom of expression should MNOs be overly zealous in their new censorship responsibilities, or use these new powers to advance private or political interests.

Terrorism national security and lawful interception

The role of intermediaries in the planning and coordination of violent acts such as terrorism is an issue that may expose intermediaries to liability. In Uganda the Anti-Terrorism Act (14 of 2002), states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news and materials that promote terrorism may be liable for the death penalty when convicted. Under the same act, any person that obstructs terrorism investigations, or interception and surveillance of communications under the act is liable to conviction and/or a fine not exceeding two years. The Regulation of Interception of Communications Act of 2010, introduces obligations to intermediaries to collect customer information (names, addresses, ID numbers), install surveillance equipment, and disclose information to authorities (when presented with a warrant or a demand from the minister). Intermediaries are obliged to assist "the monitoring centre" and ensure that their services can render real-time interception. Failure to assist the monitoring centre

47 5.3 – 5.6.
48 Under Kenya's Unified Licensing Framework,
49 Op cit, Sections 8.1 and 8.2: The guidelines state that "CSPs shall take legal responsibility for the content of political messages and must indemnify and keep indemnified MNOs. against claims that may arise out of those Political Messages" and that "CSPs shall endeavour to indemnify themselves against any claims that may arise out of Political Messages from the Political Party or individual sponsoring the Political Message."
50 This application must include the message and signed authorisation by the sponsor of the message, political party or identity documentation, and the timing of the message. Op cit, Section 4.1.
51 Op cit, Section 4.2 "Prior to the sending of any proposed Political Message and MNO shall vet its content to ensure compliance with these Guidelines. The MNO will notify the requesting entity of its decision within 18 hours of the submission of the request" and Section 4.3 "The MNO has the right to refuse the transmission of a proposed Political Message over its network that it views not to be in compliance with these Guidelines. The MNO shall give the CSP reasons for refusal."
52 4.3 to 4.6.
53 For a complete list of 83 listed CSPs, see "Content Service Providers", Communications Commission of Kenya http://cck.go.ke/mobile/licensing/register/csp.html.

is an offence, that upon conviction may result in a fine, imprisonment for up to five years, or cancellation of the intermediaries license.

In Nigeria following coordinated bomb explosions in Abuja, discussions around the role of intermediaries in being used to plan violence and terrorism begun, after for the first time in Nigerian telecom history an intermediary came under the spotlight for being used to plan violent acts of terrorism. Following this the Telecom Facilities (Lawful Interception of Information) Bill was proposed, which is currently under discussion by the House of Representatives in the Nigerian National Assembly. This bill may introduce obligations for intermediaries to cooperate with lawful interception, as well as possibly introduce liability for failure to do so.

Copyright and digital piracy

Law enforcement and public debate around digital piracy in the countries of the study, as well as in many other developing countries originally focused not on the internet or intermediaries, but rather on the distribution and sale of pirated material on CDs and DVDs. Perhaps due to increased levels of internet access in all countries, increased bandwidth and falling prices for access, digital piracy over the internet is now emerging as an issue policy and legislative debate.

In South Africa although the application of copyright law to the digital terrain is a very uncertain area.[54] In 2008, the Recording Industry of South Africa (RiSA), has sent notices to the Internet Service Providers Association of South Africa regarding three South African hosted file sharing sites, which were then removed or disabled.[55] It has been argued that "Sites that collect, index and host so-called torrents are legal in South Africa [and] protected by the constitutional right to free speech."[56] In 2009, RiSA requested that ISPA block access to block two Russian music sites that sold unlicensed/infringing mp3s. ISPA argued that it was not its responsibility to block sites.[57] Under the ECT Act intermediaries are not liable in South Africa for the transmission, storage, caching and referencing of copyright infringing content on their networks, provided that they did not create the data or initiate or modify the transmission. However this applies only to members of a recognised industry representative body. Intermediaries are have no obligation to monitor their networks for copyright infringements or police users in any way for copyright infringement (except at the request of a court). The Copyright Review Commission of the Department of Trade and Industry has recently made suggestions that a termination policy for repeat offenders should be investigated and possibly implemented.[58] This would require however amending the ECT Act as such a policy would not be legal under the current act.

In Nigeria major concerns include the increasing amount of websites on which pirated Nigerian Music and Nollywood movies are available. Digital piracy has been brought onto the legislative agenda by means of

54 See Natasha Primo and Libby Lloyd, "South Africa" In *Media Piracy in Emerging Economies* (ed. Joe Karaganis) (Social Science Research Council, 2011), 99 – 148 http://piracy.americanassembly.org/the-report/., and Department of Trade and Industry, Copyright Review Commission Report (2011), http://www.info.gov.za/view/DownloadFileAction?id=173384.

55 These sites did not provide files but rather provided links to files, much like the pirate bay. They provided links to torrents files and NBZ files (used for downloading files from Usenet). Bit Farm and NinjaCentral were both bittorrent trackers, Newshost indexed NZB files, which are files that assist computers to download multiple files from Usenet Servers.

56 enigmax, Recording Industry Takes Down BitTorrent & NZB sites, (TorrentFreak, 6 November 2008), http://torrentfreak.com/recording-industry-takes-down-bittorrent-nzb-sites-081106/; enigmax, "Recording Industry Negotiates with Bittorrent and NBZ Sites" (TorrentFreak, 24 November 2008) http://torrentfreak.com/recording-industry-negotiates-with-bittorrent-and-nzb-sites-081124/; and Rudolph Muller, "Risa and Torrent Website Truce?" (MyBroadband 24 November 2008) http://mybroadband.co.za/news/internet/6101-risa-and-torrent-website-truce.html.

57 enigmax, "ISPs refuse to block cheap russian music sites" (TorrentFreak 11 August 2009) http://torrentfreak.com/isps-refuse-to-block-cheap-russian-music-sites-090811/

58 Department of Trade and Industry, Copyright Review Commission Report (2011), Op cit.

discussions around various versions of the proposed Copyright Amendment Bill. The Copyright Amendment Bill could possibly give intermediaries obligations to disconnect repeated copyright infringer, and liability if they fail to do so. Disconnection of one's internet connect for repeated copyright infringement, as well as having human right implications, could also potentially have implications on cybercafes; meaning that they would be exposed to liability in the form of potential disconnections of their internet connection, if their users download pirated material. There are no limitations on liability for copyright infringements by third parties on their networks, although one of the versions of the proposed copyright amendment bill would have safe harbour clauses covering transmission, hosting, caching and referencing.

In Kenya during the time of the writing there was a court case concerning a mobile website WAPKid, that provides free pirated Kenyan music for mobile download.[59] Although the site is hosted in Turkey, and the domain registered with the US registrar GoDaddy[60] so the infringing site is outside of Kenyan jurisdiction, it has been alleged that mobile operators sent an SMS, encouraging users to download content from this site.[61] If this is true, then the operator(s) who sent these messages, would cease to be intermediaries, as they were actively encouraging users to download content, thus applying principles of safe harbour (if they existed in Kenyan law) would be irrelevant.

In Kenya, intermediaries have an ambiguous role with regards to copyright infringements, they are not required to monitor for copyright infringement, nor implement punitive action. They are however not protected from liability for copyright infringements.

Digital piracy and digital copyright infringement do not seem to be policy issues in Uganda, nor have their been many court cases in this regard. Uganda's safe harbour laws under the Electronic Transactions Transactions act would however possibly protect intermediaries from liability for infringing content or actions of third parties.

Arising from the research is that many artists are not aware of their rights as content creators or copyright holders, and the avenues of recourse available to them for infringements. For example in Nigeria where the Nollywood and the local industry experiences much online copyright infringements, artists do not however for example file DMCA take-down requests with YouTube, even though it would be very easy to do so.[62] In South Africa, South African Music Rights Organisation (SAMRO) and the Recording Industry of South Africa where provided by ISPA with their own specialised take-down notice form,[63] RiSA has not sent any take-down notices since 2008, and SAMRO has never sent any take-down notices.[64]

Emerging in all of these countries is a digital divide in legitimate distribution channels. For example the Music Streaming Service Spotify, and the movie streaming service Netflix are not available in any of the countries in the study.[65] Apples I-Tunes store has at the time of writing also yet to launch in South Africa. Local digital

59 The court case involves copyright holders as the plaintiffs and mobile operators as the defendants and involves the case of a mobile website based in Turkey, WAPKid.com which is offering free MP3 downloads of Kenyan music. It is alleged that certain mobile operators sent out an SMS to customers encouraging them to download from this site. For a discussion on the matter see the KICTAnet discussion thread, Music Piracy in Kenya – Government Can Help, KICTAnet mailing list 26 September 2012, http://www.kictanet.or.ke/?p=12377.

60 http://whois.domaintools.com/wapkid.com, last accessed

61 The author has no source for this, other than the discussion on the KICTAnet list, op cit.

62 http://www.youtube.com/t/copyright_notice has instructions on how to file a copyright infringement notification with YouTube.

63 Loge a RiSA Specific Takedown, http://ispa.org.za/code-of-conduct/lodge-a-risa-specific-takedown/

64 Copyright Review Commission Report (2011), Op cit. P37, Interview with Ant Brooks, former General Manager of the Internet Service Providers Association and current member of the ISPA Secretariat.

65 Although the streaming service simfy has recently launched in South Africa.

distribution channels are growing but also struggling to take traction. This is no doubt reinforced by the legislative and regulatory uncertainty with regards to content in the digital age in all countries of the study.

Conclusions arising from the research

The research has shown that debates around intermediary liability have changed over the last decade. In Nigeria the debates have gradually shifted from cybercafes and crime to telecom operators and ISPs and the issues of terrorism, copyright infringement, and digital piracy. In Kenya during the election violence hate speech particularly over mobile phones have remained central to the debate since the election violence in 2007 and in the run up to the general election in 2013.

SMS has been a focus and often the issue that often starts the debate. While SMSs are not internet content, it would make sense to include telecommunications intermediaries who bear SMSs into these debates. As content moves between SMSs and the internet, and SMSs are sent by network operators that are also internet intermediaries. Similarly, when adopting a human rights based or legal based approach, human rights and laws are the same online as they are on mobile networks, and offline

Common to all the countries in the study is that intermediaries operate in an uncertain environment with regards to the liabilities that they may possibly be exposed to. While there is some protection for intermediaries from liability in South Africa and Uganda, intermediaries in all countries in the study operate under an uncertain environment, and could be exposed to undue liability that could hamper the development of the information society and economy. This points to a need for clearer legislation in all countries regarding intermediary liability, as well as to a need for clearly legislated protection from liability for intermediaries in all countries. This can only be achieved by informing and building the capacity of all relevant stakeholders to engage in debates and advocacy around intermediary liability.

The research has served to generate knowledge on intermediary liability as well as to build the capacity of the researchers involved, the APC network and other stakeholders in understanding and researching the topic. Furthermore it has resulted in policy discussions in Kenya involving the Kenyan ICT Action Network and TESPOK.[66] Hopefully similar discussions and advocacy will be spearheaded by other researchers. The research indicates that there is a growing and ongoing interest by different stakeholders in discussing intermediary liability in Nigeria, Kenya and Uganda and a renewed interest in South Africa. Debates will continue in the next few years and possibly bring intermediary liability more prominently onto policy and legislative agendas. This follows global trends whereby new issues around intermediary liability are arising, like for example the Sinde Laws in Spain and the HADOPI laws in France, discussions around the role of intermediaries in hate speech and impersonation in India, and the Trans Pacific Partnership.[67] All stakeholders in information and communication technology and web users in these countries and the rest of the content should take advantage of this opportunity of increasing debate around this topic to involve themselves in discussions about intermediary liability, in order to shape its future on the continent.

66 The discussion took place on the 2nd of October 2012 and 10th of October 2012. See Discussion on Intermediary Liability in Kenya, KICTAnet mailing list 1 October 2012, http://www.kictanet.or.ke/?p=12486 and Defining Intermediary Liability in Kenya, KICTAnet mailing list 2 October 2012, http://www.kictanet.or.ke/?p=12513.

67 Carolina Rossini and Kurt Opsahl, "TPP Creates Legal Incentives For ISPs To Police The Internet. What Is At Risk? Your Rights." (Electronic Frontier Foundation, August 24 2012) https://www.eff.org/deeplinks/2012/08/tpp-creates-liabilities-isps-and-put-your-rights-risk.

Recommendations

- **All countries require legislated limited liability (safe harbour) for internet intermediaries.** Intermediaries must be given safe harbour under the conditions that they do not initiate or modify communications (other than in an automatic manner), that they respond to take down notices in a fair and transparent manner, that they comply with lawful requests by means of warrant or court order. While indigenous solutions are preferable to "one size fits all" approaches adopted from other legislations, a lot could be learned from CDA 230 and the DMCA safe harbour provisions in the USA, the EU E-commerce Directive, and chapter 11 of the South African ECT Act. These lessons relate both to how intermediaries are protected from liability but also how take down systems in these countries are abused. All stakeholders need to inform themselves and get involved in legislative processes. Safe harbour provisions should include all internet intermediaries and should not exclude legitimate intermediaries due to technicalities or institutional requirements. In South Africa for example limitations on liability needs to be extended beyond only members of the ISPA.
- **Protection from liability should also be extended to smaller intermediaries like cybercafes and even to individual intermediaries like blog and website owners**.
- **All countries need fair and transparent take-down procedures that are legislated and regulated.** These procedures should provide all affected parties with reasonable recourse and due process. Take-down procedures are often unduly skewed towards the complainant. Intermediaries, seeking to avoid liability are not incentivised to defend the interests of third parties (the original creators of the alleged infringing or unlawful content). Take down procedures must include mechanisms for recourse for third parties.
- **Multistakeholderism needs to be a central principle in policy and legislative debates around intermediary liability.** These debates must not just be between governments, the internet industry and copyright holders/intellectual property holders. Civil society, and content creators as well as all affected users of the internet need to get involved.
- **Termination of internet connections for repeat copyright infringements represent a human rights dilemma, access to the internet is a human right, and denying this right can have consequences on other rights like the right to free expression.** Furthermore given the importance of cybercafes and internet sharing and the fact that many cybercafes are small to medium enterprises, and often informal businesses, this imposes challenges on cybercafes, as well as an incentive or a sanction to monitor communications in order to avoid liability. Which can have implications on the right to privacy and free expression, as well as cost implications for cybercafes. Termination policies must have a punishment that fits the crime, and must balance concerns with copyright enforcement with concerns about the rights of individual users, must be sensitive to cybercafes and small businesses.
- **The mobile phone will always be important to discussions on intermediary liability in Africa.** SMS operators and SMS platforms must also be considered intermediaries, and should possibly be dealt with the same way in legislation as internet intermediaries are, and must be offered similar protections.