Intermediary Liability for Copyright Infringement

The Kenya Copyright (Amendment) Bill 2017

Walubengo J, Multimedia University of Kenya; Mutemi M, Mutemi Sumbi Law
jwalubengo@mmu.ac.ke; mercy@mutemisumbi.com

Abstract

Kenya is currently debating the Kenya Copyright (Amendment) Bill 2017, which is before parliament. In this paper a comprehensive review of the bill is made from the perspective of an Intermediary, with the view to establishing the impact it would have on their operations. It is observed that the Bill improves on the Copyright Act of 2001 by introducing the Safe Harbour regime. It is however noted that the framing of the 'Notice-Takedown' clauses require quasi-judicial skills on the part of the intermediary, which may not be appropriate. Various recommendations are suggested to improve on this and other weaknesses in the Bill.

Key Words: Intermediary Liability, Copyright, Safe Harbour, Intellectual Property

Copyright is a legal right granted to the authors of original works allowing them to exclusively control the use, exploitation and distribution of their works. Copyright infringement is conduct that violates any of the copyright holder's exclusive rights.

Direct liability for copyright infringement is imposed on the infringers themselves. Liability may also be imposed on parties who did not take part in the infringement but either has a relationship with the direct infringer or had control over the use of copyright works by the direct infringer[1]. This is referred to as secondary liability and is the bedrock of intermediary liability for copyright infringement.

Internet Service Providers (ISPs) play a crucial role in the provision of services online. Legislators are often looking for ways to on-board them to control online activity, as they reckon their efficacy would exceed that of law enforcement. What makes ISPs particularly endearing is that they have the ability to grant or deny access to their

[1] Scott, M., 2005. Safe Harbours Under the Digital Millennium Copyright Act. *NYUJ Legis. & Pub. Pol'y*, *9*, p.104

services. It is argued that they materially contribute to copyright infringement because they provide the infrastructure that the infringers use[2]. For this reason, they are in a better position than copyright holders to stop copyright infringement[3].

These conjectures may be countered thus; because of the level of automation employed by ISPs, they may not have the knowledge on the content that passes through their systems[4]. The volume of traffic also inhibits their capacity to police their users.

Intermediary liability for copyright infringement is an elusive field. Lumping ISPs as direct or secondary infringers runs the risk of curtailing investment in technological innovation for fear that the ISPs will incur liability for every conduct. On the other hand, failure to prescribe some sort of liability for copyright infringement online may discourage copyright holders from making their work available online[5].

The applicable law on copyright in Kenya is the Copyright Act of 2001 with subsequent revisions and judicial pronouncements. The Act as it is does not address the issue of intermediary liability leaving copyright holders and ISPs to determine their own modes of interaction.

Copyright (Amendment) Bill 2017

The Copyright (Amendment) Bill 2017 (the Bill) is a project of the Kenya Copyright Board established under the Act to administer all aspects of copyright and related rights in Kenya. The Bill underwent First Reading in the National Assembly on 28th September 2017 and has since been read a second time. The National Assembly is set to make committee stage amendments forthwith.

The Bill introduces substantial amendments to the Copyright Act. Of concern to this Paper are the amendments touching on intermediary liability for copyright infringement.

Internet Service Providers

The Bill defines Internet Service Providers (ISPs) as those entities *providing information services, systems, or access software provider that provides or enables computer access by multiple users to a computer server including connections for, the transmission or routing of data [sic].* This definition is compound. Unfortunately,

[2] https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-3477198-534u7t/index.html Accessed on 9th May 2018
[3] *Ibid*. p.111
[4] *Ibid*
[5] Scott, M., 2005. Safe Harbours Under the Digital Millennium Copyright Act. *NYUJ Legis. & Pub. Pol'y*, *9*, p.99.

it does not offer clarity on which internet players will be considered ISPs for purposes of the Bill.

Nevertheless, Clause 19 of the Bill which imports the safe harbour regime to our laws, alludes to various ISP conduct such as ISPs acting as providing access, caching, hosting and information location. It may be implied from the definition offered and from Clause 19 that the intention of the Bill was to co-opt all internet service providers in the fight against copyright infringement.

General Statement of Liability

The starting point on intermediary liability in the Bill is that there is no obligation on ISPs to monitor content transmitted, stored or linked. Neither is an ISP required to investigate suspicious activity for infringement[6].

An ISP will however be obliged to comply with the notice and takedown procedure which is addressed in this Paper. The ISP will also be required, pursuant to a court order, to disclose the identity of its subscribers to investigative agencies if it is suspected that those subscribers are engaging in activity that amounts to copyright infringement[7]. The third obligation is for the ISPs to designate an agent and address for receiving take down notices[8].

In addition to the broad obligations, the Bill addresses intermediary liability in two ways; prescribing safe harbours and a notice-take down procedure. These are considered in detail.

A. Safe Harbours

A key feature of the Bill is that it adopts the safe harbour regime[9]. The principle underlying safe harbours is that an ISP will be guilty of contributory or vicarious infringement if their conduct falls outside the safe harbours prescribed by law. There are four proposed safe harbours; conduit safe harbour, caching safe harbour, hosting safe harbour and information location safe harbour. The Bill borrows significantly from the American Digital Millennium Copyright Act (DMCA) 1998.

(a) Conduit Safe Harbour[10]

[6] Clause 19 introducing Section 35C(2)
[7] Clause 19 introducing Section 35C(1)(a)
[8] Clause 19 introducing Section 35C(1)(b)
[9] Clause 19
[10] Clause 19 introducing Section 35A(1)(a)

This safe harbour protects an ISP from incurring liability for infringement where the ISPs only role was to provide access to or transmit content. This extends to routing and storage of content, even in intermediate and transient cases.

The conduit safe harbour protects ISPs from general liability.

Conditions

The protection subsists as long as this conduct was undertaken in the ordinary course of business. Other conditions that must be met for this harbour to be effective are that the ISP must not initiate the transmission, select the addressee, modify the content or promote the content. This harbour is only effective where the conduct is performed in an automatic, technical manner without the selection of the content.

There is no obligation on the ISP to take down or disable access to content upon the issuance of a take down notice. This is a reasonable approach since any infringing material would be on the user's computer, the ISP in this case purely acting as a conduit for content access[11].

(b) Caching Safe Harbour[12]

The conduct targeted by this harbour is the automatic, intermediate and temporary storage of content where this is done to make the onward transmission more efficient to other recipients upon request.

Caching services are used to increase network performance and to reduce network congestion generally. Caching amounts to intermediate storage because the ISP acts as an intermediary between the originating site and ultimate user. The material in question is stored on the ISP's system for a short period of time to facilitate access by users subsequent to the one who previously sought access to it[13]. It is an integral part of the internet architecture hence demands protection[14].

The protection offered by this harbour is general- protection from liability for infringement.

Conditions

[11] Urban, J.M. and Quilter, L., 2005. Efficient process or chilling effects-Takedown notices under Section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer & High Tech. LJ*, *22*, p.13.
[12] Clause 19 introducing Section 32A(1)(b)
[13] S. Rept. 105-190 - The Digital Millennium Copyright Act of 1998, pp 42
[14] Field v. Google, Inc., 412 F.Supp. 2d 1106 (D. Nev. 2006)

This harbour only offers protection if the ISP does not modify the content, and complies with rules regarding the updating of the cache in conformity with generally accepted standards within the service sector.

There are further requirements that the ISP must comply with conditions on access to the content and that the ISP must not interfere with the lawful use of technology to obtain information on the use of the content. It is not clear what these two conditions relate to. Specifically, when the Bill requires that an ISP complies with the conditions on access to the content, it might have been useful to make reference to the conditions set out by the originating site. The term 'the lawful use of technology to obtain information on the use of material' is not clear. While this suggests a reference to non-interference with the technology that makes the content available for subsequent users, it does not offer clarity on what interference amounts to if an ISP would like to stay under the caching harbour.

There is an additional condition to the caching harbour- that the ISP must remove or disable access (it does not specify what ought to be removed or which access is to be disabled) once it receives a takedown notice or if the content has been deleted in the originating site for being unlawful content following court orders or if the content was otherwise removed. This condition refers generally to unlawful content, not copyright infringing content.

(c) Hosting Safe Harbour[15]

This harbour protects ISPs who store content at the request of a user. This may include web hosting providers, video hosting sites such as YouTube, cloud and other cloud storage providers such as Google Drive[16]. Virtual Private Servers offering hosting services to bittorent networks may also be protected under this harbour as long as they adhere to the attendant conditions[17].

The protection offered by this harbour is limited- the ISP is only protected from liability for damages arising out of the infringing activity.

Conditions

The ISP must not have actual knowledge that the content or the activity related to the content infringe on copyright. The user must not be acting under the authority or control of the ISP. There is a further condition that the ISP must not have been

[15] Clause 19 introducing Section 32A(1)(c)

[16] J Wang, DMCA Safe Harbors for Virtual Private Server Providers Hosting Bittorrent Clients accessed at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1264&context=dltr on 19th April 2018

[17] *Ibid*

aware of the facts or circumstances of the infringing activity unless the infringing nature of the content was apparent. The ISP must also comply with a takedown notice within forty-eight hours for this harbour to be effective.

(d) Information Location Safe Harbour[18]

This harbour protects ISPs if they refer or link users to a webpage containing infringing material or if the ISP facilitates infringing activity by using information location tools such as a directory, an index, reference, pointer or hyperlink. Search engines such as Google and indexing sites are protected under this harbour.

The protection offered by this harbour is limited to the liability for damages incurred.

Conditions

The ISP must not have had actual knowledge that the content is infringing content or of the facts or circumstances leading to the infringing activity unless the infringing nature of the material was apparent. Further, the ISP is required to remove or disable access to, the reference or link to the content after being notified of the infringing nature of the content or activity.

B. Notice-Take Down Procedure

The diagram below illustrates the notice-take down procedure proposed in the Bill.

Key Features

The notice-take down procedure is a two-step process only involving the complainant who claims their copyright is being infringed and the ISP who provides access to the infringing content.

[18] Clause 19 introducing Section 32A(1)(d)

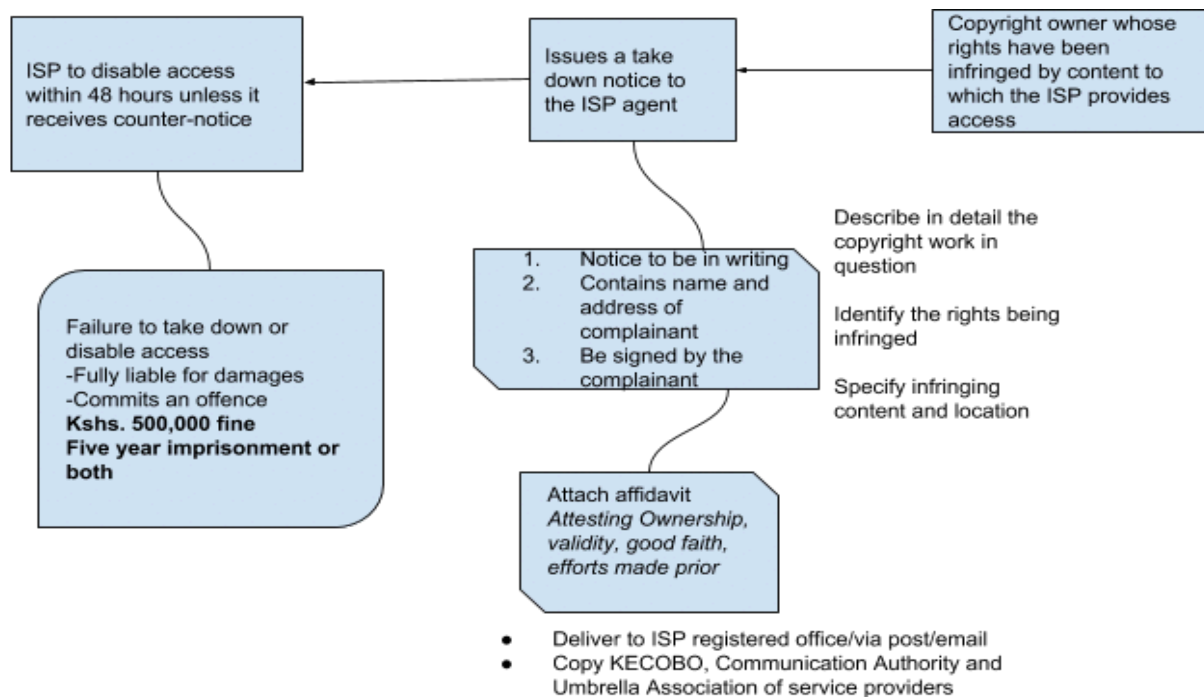

Illustration of the notice-take down procedure proposed by the Computer and Cybercrimes Bill

The complainant issues a take down notice giving the details of the infringing work, its location and the copyright being infringed.

The ISP must comply with the take down notice within forty-eight hours of receiving the notice failure to which the ISP attracts liability, both civil and criminal. Failure to comply with a take down notice is also a criminal offence on the part of the ISP attracting a Kshs. 500,000 fine or five years' imprisonment or both. These penalties are to be borne by the ISP itself and every employee of the ISP who was responsible for the non-compliance[19].

Due Process

The stance taken by the Bill ignores certain crucial aspects of due process and natural justice. Ignoring due process is likely to put the ISPs at odds with their users.

For one, the Bill transforms the ISP from a potential contributory or vicarious infringer to an arbiter[20]. The ISP, despite being the medium through which the infringement is carried out, becomes a judicial and enforcement officer contemporaneously. The ISP is to consider the affidavits sworn by the complainant, which give particulars on copyright ownership and infringement. Needless to say, ISPs are not intellectual property experts; nor are they schooled in the justice

[19] Clause 22 introducing Section 38A (1)

[20] M. Mutemi, ISPs to be Enlisted in the Fight Against Piracy in Kenya accessed at http://blog.cipit.org/2017/11/06/internet-service-providers-to-be-enlisted-in-fight-against-piracy-in-kenya/ on 19th April 2018

system, specifically on giving judicial relief. An affidavit containing untrue information would result to perjury proceedings if the same were presented before a court of law. The ISP has no interest in verifying the veracity of the statements averred in an affidavit.

The standard of proof before a complainant is granted the relief sought is extremely low and one-sided. The complainant is only required to set out specific detail of the copyright work and attach an affidavit of ownership, validity and good faith. If the take down were to be effected by a court process on an interlocutory basis, the complainant would be required to at least demonstrate that they have a prima facie case with a possibility of success and that they would suffer irreparable damage without the orders sought.

Before copyright infringement is confirmed, a claimant is required to show that the content for which copyright is claimed is copyrightable, that the complainant is indeed the copyright holder and that the defendant's conduct amounts to infringement which is not legally excused. An arbiter would thereafter make a ruling on what would be the suitable remedy in each case. Each of these issues troubles even the courts. The answers to these issues are not straightforward but rather require balancing between the complainant's and defendant's claims. The Bill bypasses these important determinations in favour of the copyright holders.

The other due process issue is the automatic granting of relief without giving the impugned content owner their right to be heard. The Bill calls for blind yet strict adherence to the take down notice by imposing criminal liability to the ISPs. The Bill mentions a counter notice[21] in passing without going into details on what an ISP is to do should they receive a counter notice. An ISP is therefore likely to ignore any such counter notice for fear of the criminal penalty to be imposed in case of non-compliance.

ISPs are offered a further incentive to indiscriminately take down content once a notice is issued- they will not be held liable for wrongful takedown in response to a valid takedown notice[22]. It only makes sense for an ISP to err on the side of

[21] Clause 19 introducing Section 35B (4)
[22] Clause 19 introducing Section 35B (9)

compliance given the promise of immunity rather than risk criminal sanction and legal fees[23]. In the process, the ISP may supress the legitimate speech of its users[24].

Registration of copyright is not mandatory in Kenya[25]. Neither is non-registration a bar to judicial action or remedy. This means that the ISPs will have no comprehensive reference point even if they were to attempt to carry out diligence to avoid customer fallout. This opens the gates for deception.

There is a foolproof mechanism introduced in the Bill to ensure that copyright holders do not abuse the notice and take down procedure[26]. However, this is limited to instances of false or malicious take down notices[27]. The dilemma in notice and take down cases however, is caused by the uncertainty on what amounts to infringement and what amounts to fair use.

Fair Use

Fair use refers to the limited use of copyright works without obtaining the permission of the author. Fair use extends to using copyright works for educational purposes, research, private use, criticism, reporting, parody, the right to quote et al[28].

Thanks to fair use, not all infringement is unlawful. Just as not every instance of infringement falls squarely within the fair use categories. This greying explains why the legislature and judiciary have developed complex rules on copyright infringement and fair use. Determinations on fair use are made on a case-by-case basis[29].

In an instance where the impugned behaviour amounts to fair use, a copyright holder still has a right to lodge a take down notice going by Clause 19. The ISP neither has the capacity nor the latitude to make a determination on what amounts to fair use. They must comply with the take down notice. A copyright holder, well aware that the activity complained of amounts to fair use, may still issue a takedown notice which the ISP ought to honour. This defeats the purpose of coming up with

[23] Walubengo J, IT Concerns in Copyright Bill https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-4311138-lbnhtv/index.html Accessed on 6th May 2018

[24] Scott, M., 2005. Safe Harbours Under the Digital Millennium Copyright Act. *NYUJ Legis. & Pub. Pol'y*, *9*, p.99.

[25] Section 22(5) of the Copyright Act

[26] Clause 19 introducing Section 35B (7)

[27] Online Policy Group v Diebold Inc. 337 F. Supp. 2d 1195 (N.D Cal. 2004)

[28] Clause 29

[29] Urban, J.M. and Quilter, L., 2005. Efficient process or chilling effects-Takedown notices under Section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer & High Tech. LJ*, *22*, p.15.

rules on fair use, which were developed to address specific social and academic concerns.

A likely outcome is the reversal of the gains offered by fair use. For instance, copyright holders issuing take down notices to silence critics or prevent their material from being mass-produced by students[30] have a right to do so under the Bill. In addition, in the notice and take down procedure, businesses have an avenue for predatory practices such as demanding the take down of their competitors' content[31].

Effect on ISP Policy

ISP policies define the relationship between an ISP and its customers. ISP policy is influenced by the legislation in place in the country of operation. Currently, platforms such as YouTube[32] employ a notice and take down in-built procedure where content may be taken down on the mere strength of a copyright infringement notice. These platforms go a step further to provide for a counter notice procedure giving accused infringers an opportunity to defend their conduct. In the YouTube example, a counter notice motivates judicial action for a formal determination on infringement. These procedures are backed up by a strike system where repeat offenders are penalized. For such platforms, change in the Kenyan legislation will not necessitate a change in policy as a stronger take down procedure is already in place.

Other providers allow the ISP to terminate its service in case a user stores, reproduces or transmits copyright infringing material. The Bill is likely to motivate policy change such that the ISPs inform their users that termination may occur in case a take down notice is lodged not upon confirmation of dealing in infringing material.

Another important policy change that may ensue is for the ISP to inform their customers that pursuant to a court order obtained under the introduced Section 35(C)(1)(a), their personally identifiable information may be surrendered to investigative agencies if they are suspected of participating in copyright infringing behaviour.

Recommendations

---

[30] *Ibid*

[31] Urban, J.M. and Quilter, L., 2005. Efficient process or chilling effects-Takedown notices under Section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer & High Tech. LJ*, *22*, p.1.

[32] https://www.youtube.com/yt/about/copyright/#support-and-troubleshooting accessed on 19th May 2018

1. Clarity

Some of the problems presented by the Bill are drafting errors that can be easily fixed.

   (a) *Clause 19 introducing Section 35A(1)(a) and (b) needs to be revisited. It is not clear whether the intention of the drafter was to exclude the ISP from all types of liability for infringement in the conduit and caching safe harbours. This can be contrasted to 35A(1)(c) and (d) which seem to limit the liability to damages. Harmonisation of this Clause is necessary.*
   (b) *Section 35A(1)(b)(v) needs clarification on what an ISP is to do on receiving a take down notice. The sub clause merely refers to 'removing or disabling access'.*
   (c) *The words unlawful and copyright infringing ought not to be used interchangeably to avoid widening the scope of the Bill. To this end, Section 35A(1)(b)(v) needs to be revisited.*
   (d) *The Bill must pronounce itself on who can issue a take down notice to the ISP. Section 35A(1)(d)(iii) demands that the ISP remove or disable access to links once the ISP has been informed of infringing content. This is not an objective test. The reference point should be upon receipt of a take down notice from the copyright holder.*

2. Technology neutral language

Legislation must be technology neutral. Technology evolves faster leaving policy and legislative processes behind to play catch up. While it is good to focus on the ISP conduct that is currently known, a better approach is for the Bill to prescribe general principles of secondary liability that will be applicable if the internet architecture changes.

3. Improving the Notice and Take Down Procedure

Due process must be written into the notice and take down procedure.

   (a) *The Bill ought to introduce an impartial arbiter to decide instances of copyright infringement.*
   (b) *The immediacy of the ISP take down is appreciated. This can be preserved. It is proposed however that the take down be temporary e.g. for fourteen days. The copyright holder must thereafter obtain a court order confirming the take down. If the copyright holder fails to obtain the court order in the given period, the ISP may restore access. This ensures that only genuine copyright holders utilise the notice and take down procedure.*

(c) The Bill must also require the ISPs to be transparent to their users on the notices received and the action taken. This gives the alleged infringers the information necessary for them to lodge a counter-notice.

(d) The counter notice ought to be elaborated. The Bill must also prescribe the form of a counter notice and what the ISP ought to do if they receive a counter notice. We propose that in the instance of a counter-notice, the ISP should not take down the impugned content; rather wait for a court order making a formal determination on the same.

4. Lessons from the DMCA

Safe harbours were first introduced into American legislation fro the DMCA (1998). The Bill essentially borrows the provisions of the DMCA. We contend that a lot of technological changes have taken place in the two decades ensuing. Further that the DMCA has been tried and tested. We must learn from the failures of DMCA and improve on those. For instance, a study carried out after the enactment of the DMCA showed that most of the take down notices sent to ISPs related to non-copyrightable material or fair use[33]. This ought to inform our position and justifies the need for an impartial arbiter before content is taken down.

[33] Urban, J.M. and Quilter, L., 2005. Efficient process or chilling effects-Takedown notices under Section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer & High Tech. LJ*, *22*, p.12.