

https://dspace.org/

Treatment of Kenya's Internet Service Providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017

Walubengo, John; Mutemi, Mercy

2019-06-28

LINK Centre, University of the Witwatersrand (Wits), Johannesburg

https://hdl.handle.net/10539/27532

Walubengo, J., & Mutemi, M. (2019). Treatment of Kenya's internet service providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017. The African Journal of Information and Communication (AJIC), 23, 1–11. https://doi.org/10.23962/10539/27532

Downloaded from a DSpace repository. https://dspace.org/

Treatment of Kenya's Internet Service Providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017

John Walubengo
Lecturer, Multimedia University of Kenya, Nairobi
https://orcid.org/0000-0001-8278-1792

Mercy Mutemi
Advocate of the High Court of Kenya, Mutemi Sumbi Law, Nairobi
https://orcid.org/0000-0002-9983-3170

Abstract
Kenya's Copyright (Amendment) Bill, 2017, is nearing its final stage of consideration by Parliament. In this article, we provide a review of the Bill's provisions in respect of its treatment of internet intermediaries, specifically internet service providers (ISPs). We seek to establish the impact that the intermediary liability provisions in the Bill could have on ISPs' operations if the Bill is passed into law in its present form. We applaud the Bill's provision for a "safe harbours" regime, whereby ISPs would incur no liability, or limited liability, for certain specific intermediary actions. However, we also note that the framing of the Bill's notice-and-takedown provisions would require quasi-judicial skills on the part of ISPs, which may not be appropriate. We conclude by providing recommendations for how legislators could address the weaknesses in the Bill's treatment of ISPs.

Keywords
copyright, copyright infringements, internet services providers (ISPs), internet intermediaries, intermediary liability, safe harbours, notice-and-takedown, Kenya, Copyright Act, Copyright (Amendment) Bill

DOI: https://doi.org/10.23962/10539/27532

Recommended citation
Walubengo, J., & Mutemi, M. (2019). Treatment of Kenya's internet service providers (ISPs) under the Kenya Copyright (Amendment) Bill, 2017. *The African Journal of Information and Communication (AJIC), 23,* 1–11.
https://doi.org/10.23962/10539/27532

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence:
https://creativecommons.org/licenses/by/4.0

1. Introduction

Copyright is a legal right granted to authors of original works allowing them to exclusively control the use, exploitation, and distribution of the 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 had a relationship with the direct infringer or had control over the use of copyright works by the direct infringer (see Scott, 2005, p. 104). This is known as *secondary liability,* and is the bedrock of *intermediary liability* for copyright infringement.

Internet service providers (ISPs) play a crucial role as intermediaries in the provision of services online (see Comninos, 2012). Legislators are often looking for ways to co-opt ISPs into controlling online activity, as they reckon the efficacy of ISPs would exceed that of law enforcement entities. What makes ISPs particularly attractive to legislators is their ability to grant or deny access to their services. Moreover, it is argued that ISPs materially contribute to copyright infringement because they provide the infrastructure that the infringers use, and that, for this reason, they are in a better position than copyright holders to stop copyright infringement (see Comninos, 2012; Ncube 2019; Walubengo, 2016). These conjectures may be countered by the argument that, because of the level of automation they employ, ISPs for the most part lack knowledge of the content that passes through their systems (see Walubengo, 2016). The large volume of traffic also inhibits ISPs' capacity to monitor the content moving to and from their users.

Intermediary liability for copyright infringement is a fraught area of copyright law. Prosecuting ISPs as direct or secondary infringers runs the risk of compelling ISPs to curtail investment in technological innovation—out of fear that they may incur intermediary liability based on a new form of conduct. At the same time, however, failure to prescribe certain forms of liability for copyright infringement online may discourage copyright holders from making their work available online (Scott, 2005). The applicable Kenyan law is the Copyright Act of 2001 (hereafter "the Act") (Republic of Kenya, 2001), with subsequent revisions and judicial pronouncements. The Act, in its present form, does not address the issue of intermediary liability, leaving copyright holders and ISPs to determine their own modes of interaction in the Kenyan context.

2. Relevant provisions in the Copyright (Amendment) Bill, 2017

Kenya's Copyright (Amendment) Bill, 2017 (hereafter the"Bill") (Republic of Kenya, 2017) is a project of the Kenya Copyright Board, which was established in terms of the Act to administer all aspects of copyright and related rights in Kenya. The Bill has undergone all the relevant stages in both the National Assembly and the Senate and, at time of finalisation of this article in June 2019, awaits final consideration

before the National Assembly. The Bill introduces substantial amendments to the Copyright Act. Of concern for this article are the amendments touching on intermediary liability for copyright infringement, and specifically intermediary liability as it pertains to ISPs.

Definition of ISPs

The Bill defines an ISP as "any person providing information services, systems, or [sic] 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;" (Clause 2). This definition is compound, and it does not offer sufficient clarity as to which internet players will be considered ISPs for purposes of the Bill. Clause 19 of the Bill, which would import the "safe harbours" regime into Kenyan copyright law, alludes to various forms of ISP conduct, such as ISPs providing access, caching, hosting and information location.

Broad ISP liability provisions

The Bill does not provide for an obligation on ISPs to monitor content transmitted, stored or linked. Neither is an ISP required, in terms of the Bill, to investigate suspicious activity for infringement.[1] An ISP will, however, be obliged to comply with the notice-and-takedown procedure provided for in the Bill. ISPs will also be required, pursuant to a court order, to disclose the identities of subscribers to investigative agencies if it is suspected that those subscribers are engaging in activity that amounts to copyright infringement.[2] A third obligation is for ISPs to designate an agent, and an address, to which notice-and-takedown instructions can be sent.[3]

In addition to these broad obligations, the Bill addresses intermediary liability in two more specific ways: (1) by prescribing safe harbours, and (2) by providing for a two-stage notice-and-takedown procedure. We now consider these two sets of provisions in detail.

Safe harbours

A key feature of the Bill is its aforementioned adoption of the safe harbours regime.[4] The principle underlying safe harbours is that an ISP will be guilty of contributory or vicarious infringement only if its actions fall outside the scope of certain permitted types of conduct ("safe harbours") prescribed by law. The Bill proposes four safe harbours: a conduit safe harbour, a caching safe harbour, a hosting safe harbour, and an information location safe harbour. The Bill's safe harbours provisions borrow significantly from section 512 of the US Digital Millennium Copyright Act (DMCA) of 1998 (USA, 1998).

1 See proposed section 35C(2) in the Bill's Clause 19.
2 See proposed section 35C(1)(a) in the Bill's Clause 19.
3 See proposed section 35C(1)(b) in the Bill's Clause 19.
4 See proposed sections 35A, 35B, and 35C in the Bill's Clause 19.

Conduit safe harbour

The conduit safe harbour, provided for in the Bill by proposed section 35A(1)(a), would protect an ISP from incurring liability for copyright infringement where the ISP's only role was "providing access to or transmitting content, routing or storage of content in ordinary course of business". Other conditions that would need to be met for this harbour to be applicable are that the ISP must "not initiate the transmission"; must not "select the addressee"; must provide the conduit "in an automatic, technical manner without selection" of the content; "must not modify" the content; and must "not in any promote" the content (sect. 35A(1)(a)(i)-(v)).

Where the conduit safe harbour applies, there would be no obligation on the ISP to take down or disable access to content upon the issuance of a takedown notice. We see this as a reasonable approach, since any infringing material would be on the user's computer and the ISP in such cases is purely acting as a conduit for content access (see Urban & Quilter, 2006).

Caching safe harbour

In terms of the caching safe harbour provided for in the Bill by proposed section 35A(1)(b), ISP conduct that would be exempt from copyright infringement liability would be content storage that is "automatic, intermediate and temporary" and conducted in order "to make onward transmission of the data more efficient to other recipients […]". ISPs generally use caching services to increase network performance and to reduce network congestion. When caching occurs, the material in question is stored on the ISP's system for a short period of time, so as to facilitate potential access by additional users seeking access to the same material. Caching is an integral part of the internet architecture, and hence it requires safe harbour exemption from liability.[5]

This harbour only offers protection if the ISP "does not modify" the content; "complies with rules regarding" cache-updating, in accordance with "generally accepted standards"; "complies with conditions on access to the material"; and "does not interfere with the lawful use of technology to obtain information on the use of the material" (sect. 35A(1)(b)(i)–(iv)). It is not entirely clear what the final two of these conditions relate to. Specifically, when the Bill requires that an ISP "complies with conditions on access" to the content, as stated in 35A(1)(b)(ii), it would have been useful to make reference to sample access conditions as set out by an originating site. And the phrase "lawful use of technology to obtain information on the use of material" is not clear. While it would seem to be a reference to non-interference with the technology that makes the content available for subsequent users, the provision does not offer clarity on what precisely amounts to "interference" of the kind that the ISP must refrain from if it is to remain in the caching safe harbour.

5 See *Field v. Google, Inc.* (2006).

There is one more condition an ISP must adhere to in order to be covered by the caching safe harbour. The ISP must remove or disable access "once it receives a takedown notice […] or where the original material has been deleted or access disabled on orders of a competent court or otherwise on obtaining knowledge of unlawful nature of the cached material" (sect. 35A(1)(b)(v)).

Hosting safe harbour

The hosting safe harbour, provided for in the Bill by proposed section 35A(1)(c), would protect ISPs from liability "for damages arising" from content they store "at the request of" a user. This could include content stored on behalf of web-hosting providers, video-hosting sites such as YouTube, cloud services, and other cloud storage providers such as Google Drive (see Wang, 2014). In order to be covered by this safe harbour, the ISP must "not have actual knowledge that the content or activity related to the material is infringing" copyright; the ISP must not be "aware of the facts or circumstances of the allegedly infringing activity unless the infringing nature of the material is apparent"; and the user must not be "acting under the authority or control" of the ISP (sect. 35A(1)(c)(i)-(ii)). Also, in order for this harbour to be effective, the ISP must comply with a takedown notice within 48 hours (sect. 35A(1)(c)(iii)).

Information location safe harbour

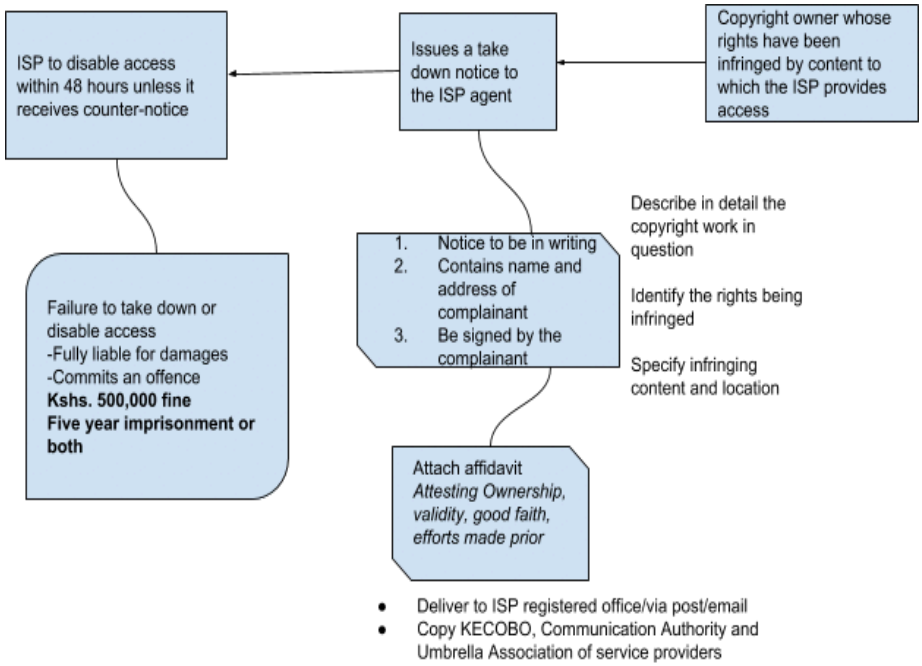
The information location safe harbour, provided for in the Bill in proposed section 35A(1)(d), protects the ISP from liability for "damages incurred by a person" if the ISP "refers or link users to a webpage containing infringing material" or if the ISP "facilitates infringing activity, by using information location tools" such as "a directory, index, reference, pointer or hyperlink". ISP facilitation of search engines such as Google, and indexing sites, is protected under this harbour. The ISP must not have had "actual knowledge" that the content is infringing, and must not have been "aware of the facts or circumstances" leading to the infringing activity (provided the infringing nature of the material was "not apparent") (sect. 35A(1)(d)(i)-(ii)). Further, the ISP is required to remove or disable access to "the reference or link to the content or the infringing activity" once it has been notified of the infringing nature of the content or activity (sect. 35A(1)(d)(iii)).

Notice-and-takedown procedure

The diagram below in Figure 1 illustrates the notice-and-takedown procedure proposed in the Bill (sect. 35(B)(1)). The notice-and-takedown procedure would e a two-step process involving (1) the complainant who claims its copyright is being infringed, and (2) the ISP who is providing access to the infringing content. The complainant must issue a takedown notice giving the details of the infringing work, its location, and the copyright being infringed. The ISP must comply with the takedown notice within 48 hours of receiving the notice, with failure to do so resulting in liability, both civil and criminal, for the ISP. In respect of the criminal liability, failure to comply with a takedown notice would attract a KES500,000 (approx. USD5,000)

fine, or a five-year imprisonment, or both. These penalties would be borne by the ISP and by every employee of the ISP who was responsible for the non-compliance with the takedown notice.[6]

Figure 1: Illustration of the notice-and takedown procedure proposed by the Bill



Source: Authors' illustration

The Bill's approach to notice-and-takedown ignores certain crucial aspects of due process and natural justice. Ignoring due process is likely to put the ISPs at odds with their users. The Bill would, if signed into law in its present form, transform the ISP from a potential contributory or vicarious infringer to an arbiter (see Mutemi, 2017). The ISP, despite being the medium through which the infringement is carried out, would become, contemporaneously, a judicial and enforcement officer. The ISP would be required to consider the affidavits sworn by the complainant, which give particulars on copyright ownership and infringement.

6 See proposed section 38(A)(1) in the Bill's Clause 22.

Needless to say, ISPs are not intellectual property experts; nor are they schooled in the justice system, specifically on matters of giving judicial relief. An affidavit containing untrue information would result in perjury proceedings if the same were presented before a court of law. Yet the ISP has no interest in verifying the veracity of the statements averred in an affidavit. Thus, the standard of proof required before a complainant is granted relief sought would be extremely low and one-sided if the Bill were to become law without amendment. The complainant would only be required to set out specific details of the copyright work and attach an affidavit of ownership, validity, and good faith.[7]

If the takedown were, more correctly, to be effected by a court process on an interlocutory basis, the complainant would be required to at least demonstrate that it (1) has a prima facie case with a possibility of success, and (2) that it would suffer irreparable damage without the orders sought. In the Kenyan legal context, before copyright infringement is confirmed, a claimant is, in terms of the precedent established by *Paul Odalo Abuor v Colourprint Ltd & Text Book Centre Ltd* (2002), required to (1) show that the content for which copyright is claimed is copyrightable, (2) that the complainant is indeed the copyright holder, and (3) that the defendant's conduct amounts to infringement that 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 questions are not straightforward, and rather require balancing between the complainant's and defendant's claims. The Bill's provisions would bypasses these important determinations, thus privileging the claims of copyright holders.

The other due process issue raised by the Bill's approach to notice-and-takedown is the automatic granting of relief without giving the impugned content owner its right to be heard. The Bill provides for blind, strict adherence to the takedown notice, through imposing criminal liability on ISPs failing to execute takedown notices. The Bill cites a counter-notice provision in proposed section 35B(4), but only in passing and without going into detail as to what an ISP would be required to do should it receive a counter-notice. An ISP could, therefore, be expected to ignore any such counter-notice for fear of the criminal penalty to be imposed in case of non-compliance with the original takedown notice.

ISPs are offered a further incentive, in the Bill's proposed section 35B(9), to indiscriminately take down content once a notice is issued, because, in terms of this section, they will not be held liable for wrongful takedown in response to a valid notice-and-takedown procedure. It would only make sense for an ISP to err on the side of compliance, given the promise of immunity, rather than risk criminal sanction

7 See proposed section 35B(2)(g) in the Bill's Clause 19.

and legal fees (Walubengo, 2018). In the process, the ISP could supress the legitimate speech of its users (see Scott, 2005, p. 99).

Registration of copyright is not mandatory in Kenya.[8] Neither is non-registration a bar to judicial action or remedy. This means that ISPs would have no comprehensive reference point, even if they were to attempt to carry out due diligence in order to avoid customer fallout. This would open the gates for deception, i.e., false copyright claims leading to erroneous content takedowns. The Bill provides a checking mechanism, in proposed section 35B(7), to ensure that copyright holders do not abuse the notice-and-takedown procedure, but this mechanism is limited to instances of false or malicious notice-and-takedown instructions.

Exceptions and limitations

Another potential dilemma for the Bill's proposed in notice-and-takedown procedures is the uncertainty, in the Kenyan legal context, as to which conduct would amount to non-infringing use because of its coverage under the limitations and exceptions provided by Kenyan copyright law. The "fair dealing" exception, provided for in the Act and in the Bill's Second Schedule (section 26(3)(A)(1)(a)), permits use of copyright works, without obtaining the permission of the right holder, for "fair dealing for the purposes of scientific research, private use, criticism or review, or the reporting of current events; […]". In terms of this provision, and other limitations and exceptions provided for in the Act and the Bill, not all unauthorised use of copyrighted works is unlawful. At the same time, however, it is often debatable whether a use of a work is permitted by one of the limitations and exceptions. These grey areas are why governments and judiciaries have had to develop complex regulations and rules on fair dealing and other limitations and exceptions, with determinations often having to be made on a case-by-case basis (see Urban & Quilter, 2006).

In terms of the Bill, in an instance where an impugned behaviour amounted to fair dealing or a use permitted by another limitation or exception, a copyright holder would still have a right to commence a notice-and-takedown procedure (35(B)(i)). Yet ISPs cannot be expected to have the capacity to make a determination on what amounts to a permitted use in terms of the copyright limitations and exceptions, and they will be incentivised, if the provisions in the Bill become law, to comply with takedown notices. A copyright holder, even if well aware that the activity complained of amounts to fair dealing, could still be inclined to issue a takedown notice, knowing that the ISP will almost certainly honour it. This would defeat the purpose of development of the fair dealing exception and other copyright limitations and exceptions, which were developed to ensure public-interest access in support of access to knowledge and related educational and social imperatives. A likely outcome

8 See section 22(5) of the Copyright Act of 2001.

would be reversal of gains offered by the fair dealing exception. For instance, copyright holders would have a right, under the provisions proposed by the Bill, to issue takedown notices in efforts to silence critics (see Urban & Quilter, 2006).

An additional concern with Bill's proposed notice-and-takedown procedure is the apparent latitude it would provide businesses to engage the predatory practice of demanding takedown of a competitor's content (see Urban & Quilter, 2006).

3. Recommendations

Learn from the US experience

Safe harbours were first introduced into American legislation by the DMCA of 1998, and the Kenyan Bill essentially borrows the provisions of the DMCA. Numerous technological changes have taken place in the two decades ensuing since the DMCA's enactment, and, moreover, the DMCA has been tried and tested, with its weaknesses demonstrated. Kenya must learn from the failures of DMCA and improve on the DMCA model. For instance, a study carried out after the enactment of the DMCA showed that most of the takedown notices sent to ISPs related to non-copyrightable material or materials covered by "fair use" (the US variant of "fair dealing", which is more flexible than fair dealing) (Urban & Quilter, 2006).[9] This finding needs to inform the Kenyan position, i.e., it shows the need for an impartial arbiter to play a role in decisions as to whether content should be taken down.

Add clarity

Some of the problems presented by the Bill are drafting errors that can be easily fixed, as follows:

- Clause 19, introducing sections 35A(1)(a)-(d), needs to be revisited, as its present wording exempts ISPs from general liability for copyright infringement for conduct covered by the *conduit* and *caching* safe harbours (sect. 35A(1)(a)–(b)), yet the exemption from liability is only for "damages" in respect of conduct covered by the *hosting* and *information location* safe harbours (35A(1)(c)-(d)). Harmonisation would appear to be necessary across 35(A)(1).

- Section 35A(1)(b)(v) needs refinement in order to state more precisely what an ISP is to do upon receiving a takedown notice. At present, the sub-section refers, too vaguely, to "removing or disabling access".

- The Bill must pronounce itself more precisely on who can issue a takedown notice to an ISP. The Bill's proposed Section 35A(1)(d)(iii) would require that the ISP remove or disable access to links once the ISP has been informed

9 See *Online Policy Group v Diebold Inc.* (2004), a US case that demonstrates illegitimate use of notice-and-takedown procedures in violation of "fair use" doctrine provisions for permission-free use of copyright works.

of infringing content. We recommend that this requirement be made more reliable through specification that whoever is informng the ISP of infringing content must be the proven copyright holder for the material.

Improve the notice-and-takedown procedure

Due process must be written into the notice-and-takedown procedure, via the following changes:

- The Bill ought to provide for an impartial arbiter to decide on instances of copyright infringement.
- The need for immediacy of the ISP takedown is appreciated, and this can be preserved. We propose, however, that the takedown be temporary e.g., for 14 days, during which time the copyright holder would have to obtain a court order confirming the necessity of the takedown, i.e., confirming that the takedown arose out of a genuine infringement. If the copyright holder fails to obtain the court order in the given period, the ISP could restore access to the content. This would help ensure that there is only genuine use of the notice-and-takedown procedure.
- The Bill must also require ISPs to be transparent to their users on the notices received and the actions taken. This would give alleged infringers the information necessary for them to lodge counter-notices.
- The counter-notice provisions ought to be elaborated. The Bill must also prescribe the form of a counter-notice, and what the ISP ought to do if it receives a counter-notice. We propose that in the instance of a counter-notice, the ISP should not be compelled, at the same time, to take down the impugned content in terms of the original notice; rather, the ISP should be compelled to wait for a court order making a formal determination on the same.

References

Legal instruments and cases

Field v. Google, Inc., 412 F. Supp. 2d 1106 (D. Nev. 2006).

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

Paul Odalo Abuor v. Colourprint Ltd & Text Book Centre Ltd (2002) (unreported).

Republic of Kenya. (2001). Copyright Act of 2001, as amended in 2009. Retrieved from http://www.kenyalaw.org/Downloads/Acts/Copyright%20Act.pdf

Republic of Kenya. (2017). Copyright (Amendment) Bill, 2017. Retrieved from http://www.parliament.go.ke/sites/default/files/2018-09/COPYRIGHT%20%28AMENDMENT%29%20BILL.pdf

United States of America (USA). (1998). Digital Millennium Copyright Act (DMCA) of 1998. Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998). https://www.copyright.gov/legislation/pl105-304.pdf

Secondary sources

Comninos, A. (2012). *The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain*. Association for Progressive Communications (APC). Retrieved from https://www.apc.org/en/pubs/liability-internet-intermediaries-nigeria-kenya-so

Mutemi, M. (2017). ISPs to be enlisted in the fight against piracy in Kenya. [Blog post]. Centre for Intellectual Property and Information Technology (CIPIT), Strathmore University. Retrieved from http://blog.cipit.org/2017/11/06/internet-service-providers-to-be-enlisted-in-fight-against-piracy-in-kenya/

Ncube, C. (2019). Submission on the South African Copyright Amendment Bill [B13B - 2017]. Submitted to NCOP Select Committee on Trade and International Relations, Parliament of South Africa, Cape Town, on behalf of DST/NRF SARChI Research Chair: Intellectual Property, Innovation & Development, University of Cape Town. Retrieved from http://infojustice.org/wp-content/uploads/2019/03/Ncube-NCoP-Submission-February-2019.pdf

Scott, M. (2005). Safe harbours under the Digital Millennium Copyright Act. *NYU Journal of Legislation & Public Policy*, *9,* 99–166. Retrieved from http://www.nyujlpp.org/wp-content/uploads/2012/11/mike-scott-safe-harbors-under-the-digital-milennium-copyright-act.pdf

Urban, J. M., & Quilter, L. (2006). Efficient process or "chilling effects"? Takedown notices under section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer and High Technology Law Journal*, *22*(4), 621–693. Retrieved from https://scholarship.law.berkeley.edu/facpubs/501/

Walubengo, J. (2016, December 6). How the internet has made copyright protection murkier. [Blog post]. *Daily Nation.* Retrieved from https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-3477198-534u7t/index.html

Walubengo, J. (2018, February 19). Key IT concerns in copyright bill. [Blog post]. *Daily Nation.* Retrieved from https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-4311138-lbnhtv/index.html

Wang, S. J. (2014). DMCA safe harbors for virtual private server providers hosting BitTorrent clients. *Duke Law & Technology Review*, *12*, 163–181. Retrieved from https://scholarship.law.duke.edu/dltr/vol12/iss1/9/