Treatment of Kenya's Internet Intermediaries under the Computer Misuse and Cybercrimes Act, 2018

John Walubengo
Lecturer, Multimedia University of Kenya, Nairobi

Mercy Mutemi
Advocate of the High Court of Kenya, Mutemi Sumbi Law, Nairobi

Abstract
Kenya has this year enacted the Computer Misuse and Cybercrimes Act, 2018. This article reviews the Act from the perspective of internet intermediaries, with a view to establishing the impact the Act is expected to have on intermediaries' operations. The article outlines key concerns regarding the Act's provisions in respect of obligations and liabilities of intermediaries, particularly with regard to obligations to support state agencies. Recommendations are made for how the Act could be amended to cater more optimally to both state and intermediary concerns.

Keywords
Computer Misuse and Cybercrimes Act, Kenya, internet intermediaries, intermediary liability, cybercrime

DOI: https://doi.org/10.23962/10539/26114

Recommended citation
Walubengo, J., & Mutemi, M. (2018). Treatment of Kenya's internet intermediaries under the Computer Misuse and Cybercrimes Act, 2018. *The African Journal of Information and Communication (AJIC)*, *21*, 1–19. https://doi.org/10.23962/10539/26114

Acknowledgement
Funding for the research presented in this article was provided by the African Academic Network on Internet Policy (AANoIP).

1. Introduction

The internet landscape in Kenya has undergone a profound transformation. Gone are the days of control by a single monopoly offering an inadequate, failure-prone and expensive internet (Ndemo & Weiss, 2016, p. 35). The internet is now a transformative agent that has permeated every economic activity in the country, while redefining the dynamics of social engagement.

According to the Communications Authority (2018), Kenya has 51.1 million internet users, a penetration level of 112.7%.[1] This ubiquity comes, however, with an increase in cybercrime incidents targeting the government, financial institutions, telecommunication entities, individuals, and online platforms. The cost of cybercrime in Kenya in 2017 was estimated at KES21 billion (Serianu, 2017). Where this problem has arisen in other jurisdictions, governments have stepped in to regulate online behaviour and punish bad actors. Kenya's regulatory attempts have seen the enactment of the Computer Misuse and Cybercrimes Act, 2018 (hereinafter the "2018 Act"). This article critically examines the provisions of this Act in respect of the obligations and liability it imposes on internet intermediaries.

2. Legislative context

The 2018 Act is not the first legislative attempt by the Kenyan government to control activities in the information and communication technology (ICT) space. In 1998, the Kenya Communications Act promised a new dawn for the telecommunication industry. That Act of 1998 liberalised the telecommunications sector out of the monopoly of the former Kenya Posts and Telecommunications Corporation, a government monopoly that was unable at the time to provide telephone services to a majority of the population (Republic of Kenya, 1998a). While encouraging privatisation and investment in the telecommunications sector, the Act also dwelled substantially on the issue of licensing, including matters of liability of licensees, thus marking the beginning of regulation of intermediaries. The issue of illegal use of communications infrastructure arose when that 1998 Act was under consideration. The lawmakers' concern at the time was the tapping of telephones (Republic of Kenya, 1998a).

A decade later, in 2008, the country's focus had shifted from telephone and postal services to crafting a more comprehensive ICT and e-commerce framework (Republic of Kenya, 2008). Kenya was, at the time, recovering from its post-election violence of late 2007 and early 2008, and there was consensus that messages spread via text and online had not only catalysed ethnic hatred but also rallied mobs to participate in the ensuing violence (Cheeseman, 2008). The 1998 Act was thus amended in 2008 to

1 Estimated internet penetration exceeds 100% due to many Kenyans having more than one internet connection, i.e., internet penetration is calculated in terms of the combined total number of mobile data/internet subscriptions, terrestrial wireless subscriptions, and fibre optic and satellite subscriptions.

address these challenges by publishing regulations on the prevention of transmission of undesirable bulk political messages. Matters of intermediary liability arose again in 2013 via the Kenya Information and Communications (Amendment) Act, 2013, which required mandatory registration of mobile phone subscribers (Republic of Kenya, 2013). Yet another key development at this stage was the amendment of the Evidence Act of 1963 to allow courts to admit electronic material into evidence (Republic of Kenya, 1963).

Simultaneously, the National Cohesion and Integration Act, 2008 was passed (Republic of Kenya, 2008b). By it, the legislature began prescribing content offences. The offences of hate speech (sect. 13) and ethnic or racial contempt (sect. 62) in the National Cohesion and Integration Act can be seen as targeting primary offenders. However, the Act's use of the words "distribute", "publish" and "provide", in describing the actions that can lead to the offence of hate speech, leave some latitude for inclusion of intermediaries as offenders as well. Further, Section 62(2) of that Act provides for the offence of ethnic or racial contempt as a strict liability offence by "media enterprises", without offering further guidance on what a media enterprise is. And section 57 creates the compliance notice system whereby the National Cohesion and Integration Commission can demand that an intermediary disrupt access to impugned material.

Currently, offences committed over the internet are dealt with under the Kenya Information and Communications Act (KICA), 1998 and the Penal Code. The offences under KICA are tripartite: offences by the intermediaries themselves, offences against the investments made by intermediaries, and substantive offences arising out of the use of computer systems. This third category criminalises unauthorised access to, interception of, and interference with, computer systems, and goes a step farther to prescribe two content offences: improper use of a system, and obscene publication. The High Court of Kenya has since declared, in a 2016 ruling, the first of these two, the offence of improper use of system, unconstitutional, casting doubt on whether the latter would hold if challenged in court.[2] Most of these offences are repealed by section 69 of the 2018 Act. The investigation procedures under Part VII of the Act relate to investigations of entities providing telecommunication services without licences. The Act is quiet on the role of intermediaries in investigation of content offences and misses an opportunity to delimit the extent of intermediary liability.

The Penal Code is applicable to online conduct that is forbidden offline and for which a penalty is spelt out in the Code. This exemplifies (see Best, 2004) the internet governance maxim that says what is illegal offline is illegal online, hence no need to come up with a new offence to cover online conduct.

2 See *George Andare v the Attorney General & 2 Others* [2016].

3. Computer Misuse and Cybercrimes Act, 2018

In its recital, the 2018 Act spells out its purposes as: to provide for offences relating to computer systems; to enable timely and effective detection, investigation and prosecution of computer crimes and cybercrimes; and to facilitate international cooperation in dealing with computer and cybercrime matters. To these ends, the Act introduces several offences.

The first category of offences comprises unauthorised access,[3] access with intent to commit a further offence,[4] unauthorised interference,[5] unauthorised interception,[6] provision and use of illegal devices and access codes,[7] and unauthorised disclosure of passwords.[8] These offences are standard in cybercrime legislation (see ITU, 2017; Council of Europe Budapest Convention, 2001).

Most of these offences were not provided for in KICA. Neither do they fit into the categories of offences of stealing, robbery, breaking and entering, and false pretences that are provided for in the Penal Code. Criminalising such conduct can therefore be welcomed by all internet users, including intermediaries who often find themselves victims of cybercrime (*Business Daily*, 2018).Through the Act, offending online conduct can now form the basis of a sustainable criminal charge.

Sections 20 and 21 of the 2018 Act give intermediaries additional reasons to be happy. Section 20 imposes an enhanced penalty when the offence involves a "protected system", i.e., a system for the provision of communication and financial services and payment systems. Section 21 creates the offence of "cyber espionage", which ought to insulate intermediaries from predatory business practices by competitors, and from espionage as a service (EaaS). EaaS is an emerging threat that allows hackers to lease attack tools from the cloud rather than create them from scratch.

The second category of offences introduced by the Act is content offences. Section 22 makes it a crime to publish false information with the intent that the information be acted on as authentic. Freedom of expression as guaranteed in Article 33 of the 2010 Constitution of Kenya protects publication of all kinds subject to the limitations listed in Articles 33(2)[9] and (3).[10] The section, while well-intended, falls

3 Section 15.
4 Section 15.
5 Section 16.
6 Section 17.
7 Section 18.
8 Section 19.
9 The right to freedom of expression in the Constitution does not extend to propaganda for war, incitement to violence, hate speech or advocacy of hatred that constitutes ethnic incitement, vilification of others or incitement to cause harm; or is based on any ground of discrimination specified or contemplated in Article 27(4).
10 According to the Constitution, in the exercise of the right to freedom of expression, every person shall respect the rights and reputation of others.

outside the scope of allowable limitations to freedom of expression. Another glaring shortcoming of this Section is the failure to define what constitutes publication. Clarity to this end would shield intermediaries from secondary liability that often arises in content offences (Dinwoodie, 2017).

Sections 24 of the Act sets out the offence of child pornography. This is an improvement on section 16 of the Sexual Offences Act, 2006 (Republic of Kenya, 2006). Unlike the latter, the 2018 Act forbids the delivery, transmission, or distribution of the material in question, or making the same available in any way. Also forbidden is the possession of child pornographic material in a computer system or computer data storage medium. This general proscription may present problems for intermediaries, although a majority of intermediaries already have a zero-tolerance policy towards child pornography (Technology Coalition, 2015).

The 2018 Act also addresses the offences of computer forgery and computer fraud. The elements of computer forgery under section 25 are sufficiently comprehensive to cover social-engineering attacks. Section 26 creates the offence of computer fraud. The harassment offences of cyberstalking and cyberbullying are included in section 27 of the Act—a laudable inclusion to prevent internet users from conduct that has detrimental effects on victims as described by (Englander et al., 2017).

Part IV of the Act lays out the investigation procedures to be undertaken in obtaining evidentiary material in computer systems, subscriber information, traffic data and content data. Part V addresses international cooperation in cybercrime investigations. These two parts are discussed in detail later in this article.

4. Intermediary liability

An exposition on cybercrime is incomplete without detailing the role of intermediaries. Crimes committed over the internet are difficult to detect and prosecute. For one, delinquent internet users enjoy anonymity which can be achieved in various ways. These vary from the use of pseudonyms and encryption, the use of virtual networks and proxy servers to mask internet protocol (IP) addresses, and the deletion of posts and clearing of cookies and browser history (Rainie, 2013). Second, security threats are now extremely complex, ranging from data interception, data interference, and illegal access to systems, to installation of spyware, data corruption, sabotage, denial of service, and identity theft (Kurbalija, 2016). Further, cybercriminals have graduated to using botnets, targeting cloud storage, and using the internet of things (IoT) to carry out large-scale attacks. This makes it problematic and costly for enforcement officers to identify the offenders, collect evidence, and prosecute the direct offenders (Kreimer, 2006). Consequently, governments have changed tactics, shifting from only going after direct offenders to imposing liability on intermediaries and further enlisting them to net the direct offenders.

This article adopts the description of intermediaries offered by Perset (2010) and MacKinnon (2015), whereby intermediaries are entities which: (1) give access to, host, transmit, and index content, products and services originated by third parties on the internet, or (2) provide internet-based services to third parties. This definition includes internet service providers (ISPs), data-processing and web-hosting providers, internet search engines and portals, e-commerce platforms, social networks, online communities, and blogging services (MacKinnon, 2015, p. 21). It is possible to delineate the extent of liability imposed on intermediaries into three categories: strict liability, conditional liability, and broad immunity (MacKinnon, 2015, p. 40). Different modes of liability are levied for different offences. These modes also differ according to the jurisdiction.

5. How the 2018 Act addresses intermediary liability

Strict intermediary liability is imposed when the mere fact of providing access to illegal content incriminates the intermediary. Section 24 of the Act, which creates the offence of child pornography, hints at strict liability, but, as discussed below, this may be in conflict with section 56, which gives an overarching direction on intermediary liability.

It is opined that strict liability inevitably leads to excessive monitoring and censorship by intermediaries (Hornik & Villa llera, 2017). Intermediaries are likely to refuse to carry content that closely resembles forbidden categories, even where the illegality is debatable. This poses a risk to freedom of expression. For an intermediary to escape liability under the strict-liability principle, it has to proactively monitor all the content accessible to users in a certain jurisdiction, distinguish between legal, illegal and questionable conduct, constantly filter the content, and disrupt the activities likely to give rise to liability for the intermediary in that jurisdiction. The reverse may also be true, unfortunately: Failure to impose strict liability may act as a disincentive to proactive monitoring on the part of the intermediary.

Conditional liability

Under a conditional-liability regime, intermediaries are exempt from liability if they abide by certain conditions laid out in law. This liability regime is an extrapolation of the tortious principle of vicarious liability (Sloot, 2015). Under vicarious liability, an intermediary would be held accountable if it had knowledge of any illegal activity carried out using its resources, had the ability to exercise control to stop the illegal activity, and stood to benefit in one way or another from the illegal activity. Conditional liability is the foundation of the celebrated "safe harbours" protection. (A "safe harbour" protection exempts an intermediary from liability if the intermediary abides by certain rules.) This seems to be the approach taken by section 56 of the Act, which gives the conditions that would give rise to civil and criminal intermediary liability. We note, however, that section 56 is not specific enough on what these

conditions are. This is likely to present difficulties for law enforcement and for the courts when inferring intermediary liability.

The third category of intermediary liability cited above, broad immunity, accords the intermediaries the protection under conditional liability and goes a step further, allowing them to come up with a content policy. If the intermediaries disrupt activities based on this content policy, they are protected from liability. For instance, pulling down content violating their content policy will not be termed a violation of their users' freedom of expression. Broad immunity is not adapted in the Act.

Section 56 of the Act provides a general statement on intermediary liability. An intermediary will attract civil or criminal liability if it had actual notice or actual knowledge of an offence, or if the intermediary wilfully and with malicious intent facilitated the commission of the offence. If by a mere omission or failure to act the intermediary facilitated, aided or abetted the commission of the offence, no liability will attach. It is unclear from the Section at what point actual notice and knowledge become a determining factor for liability. For instance, if an intermediary learns of an offence *ex post facto*, does this count as actual knowledge for which the intermediary will be liable? The section also fails to offer an absolution route for the intermediary. Should the intermediary learn of an impending offence over which it has no control, what should the intermediary do to excuse itself from liability? Further, where an intermediary has been made aware of unlawful content and fails to take action to disrupt access, does this constitute knowledge and wilful action for purposes of subsequent prosecution?

Section 56(2) absolves intermediaries from liability for maintaining and making available the provision of their service. This override comes close to the renowned safe harbours which are a list of the core functions of intermediaries that would be exempted from liability. Without such a wholesale exemption from liability, criminal liability may be imposed on a case-to-case basis, usually by arbiters who may not appreciate the intricacies and roles of each internet intermediary.

Reading sections 56(1) and (2) together leads to the conclusion that the Kenyan position is that intermediaries will not be held responsible for any unlawful conduct unless it can be shown they had actual notice or actual knowledge of the conduct or that they acted wilfully and with malicious intent to facilitate the unlawful conduct. There are several other sections in the Act that tease intermediary liability without stating as much. One such section is section 42, which makes it an offence to knowingly and wilfully aid or abet the commission of any offence under the Act. The *men rea* elements of this offence are "knowledge" and "wilful action", just as in section 56.

Notice and knowledge

What amounts to actual "notice" and actual "knowledge" is a controversial issue in itself. It is often argued that intermediaries have knowledge and control of, or have the ability to monitor, the content they provide access to (Article 19, 2013). Such a stance fails to take into account the fact that it is economically and technically infeasible for intermediaries to monitor all the activity taking place over the internet (Truyens & Van Eecke, 2016). Further, such large-scale monitoring of, and blocking of access to, content may lead to a "chilling effect", whereby intermediaries, afraid of the consequences of non-compliance or that their conduct will lead to unforetold liability, may resort to broad censorship and blocking and in the process disrupt access to lawful content (Truyens & Van Eecke, 2016, p. 6).

The other issue pertaining to knowledge and notice is the matter of what precisely amounts to knowledge by the intermediary. Courts would have to contend with whether knowledge by any personnel at the intermediary is enough to implicate the intermediary, or whether there is a designated officer of the intermediary who must have had knowledge for liability to attach.

Publication

Two other sections in the Act invoke intermediary liability: section 24 on child pornography and, by extension, sections 22 and 23 on false publications. What is problematic in section 24 is its definition of publication to include "making available in any way". Sections 22 and 23, meanwhile, use the word "publish" but fail to define the parameters of the word in the context of those two sections. Following the principles of statutory interpretation, it is possible that the courts will look to section 24 to define publication under sections 22 and 23. Section 24 also extends criminal liability to entities that have, in their possession or custody, child pornography materials. Intermediaries offering cloud storage facilities may be netted under this section.

What these sections in the Act mean to search engines, in particular, needs further examination. Two aspects of search engines are of concern: caching and dissemination (Gürkaynak, 2013). Both of these functions are carried out in a technical, automatic, and passive manner. It would therefore be untenable to demand that search engines be obliged to consider the legality of a website that they make available in their search results. This would also be inconsistent with international judicial precedent on the legal liability of search engines.[11]

Nonetheless, it does not seem that search engines would escape liability under section 24. Whereas search engines are not publishers in the traditional sense,[12] it

11 See *SARL Publison System v SARL Google France*, Court of Appeal, Paris (19th March 2009); and *Jensen v Google Netherlands*, District Court of Amsterdam (26 April 2007).

12 See *Perfect 10 v. Google, Inc.*, 78 U.S.P.Q. 2d 1072 (C.D. Cal. 2006).

may be argued that they do indeed "make content available" which would make them publishers under section 24 of the Act. To avoid liability, a search engine would have to make sure that none of its ranked and listed links are to a site containing pornographic material as contemplated in section 24(3) of the Act. An alternative legislative approach that would achieve the same result without disproportionately burdening search engines would be to extend immunity to the search engines as long as they are unaware that a website whose link they have listed is illegal. This may be cured by section 56(2). How sections 24(1) and 56(2) co-exist will be a matter for judicial interpretation.

Critical information infrastructure

The Act establishes the National Computer and Cybercrimes Co-ordination Committee, which will be made up of public officers drawn from various government offices. The Committee will designate certain systems, deployed in the health, energy, financial and security sectors, as critical infrastructure (sect. 9). Designation as critical infrastructure comes with additional responsibilities to the intermediaries in charge of the systems. For one, these intermediaries will be subjected to an additional level of regulation by the Committee. Secondly, these intermediaries will be required to report any cybercrime threats to the system to the Committee. In addition, a compliance report is to be submitted to the Committee. Failure to comply with these requirements constitutes an offence.

Investigation procedures

Part IV of the Act addresses investigation procedures. Often, investigation procedures run afoul the right to privacy, which is guaranteed under Article 31 of the Kenyan Constitution. A lack of clear-cut procedures also subjects intermediaries to an unpredictable governance environment, which may sour customer relations and open up the intermediaries to lawsuits. What we see in Part IV is an added responsibility to intermediaries.

Section 48 outlines the search-and-seizure procedure, which involves getting a warrant from a court. A court may grant a warrant to search a premises once it is satisfied that there is a plausible reason that data therein would help in the investigation of a crime or was acquired criminally. This section fails to take into account that when it comes to digital evidence, the search warrant ought to take care of two things; the physical search of the premises to seize hardware that may have been instrumental in committing a crime and an electronic search to obtain data from the seized hardware (Kerr, 2005). A mere search on the premises does not give police officers the permission to obtain information located in computer hardware. A better approach would be to include in the preconditions for granting a warrant that the police officers ought to identify the evidence to be sought at both the physical and electronic search stages. The search warrant described in this section would also not be adequate where the evidence is stored in a cloud.

According to section 49(2), the owner of the seized system may be allowed some leeway to access and copy the information in the seized system. This is not guaranteed however as the police officers have the right to refuse access. This raises concerns for business operations. Investigations take time. Such a refusal would ground an entity and in fast paced sectors, render them redundant. Extended retention with no access also raises a constitutional issue as it affects the right to own property (in Article 40 of the Constitution).

Police officers will have the right, subject to judicial approval, to co-opt service providers in their investigations as per section 52(1)(b)(ii). This opens up intermediaries to corporate espionage. The Directorate of Criminal Investigations has a digital forensic lab with equipped forensic examiners. This is the office that ought to assist the police officers in investigations.

Intermediaries will not be liable for the disclosure of any information if the disclosure is made pursuant to the Act. Some of the orders compelling intermediaries to release certain information to police officers may be accompanied by a gag order. The gag order will require the intermediary to keep confidential the existence of any such orders and the extent of the intermediary's cooperation in the investigation. The relationship between intermediaries and their customers is one of trust. Full disclosure on what the intermediary has done to co-operate with the government would boost this trust. The 2001 Budapest Convention on Cybercrime, in its Article 16, proposes that details on the extent of the intermediaries' cooperation with the government be kept confidential but only for a certain period of time (Council of Europe, 2001). It is indeed necessary to keep this information confidential for a given period of time to protect the integrity of an investigation. Beyond that, intermediaries should be free to disclose to their customers that their information was shared with law enforcement.

Service providers

The Act imposes obligations on service providers. For purposes of the Act, a service provider is defined as "a public or private entity that provides to users of its services the means to communicate by use of a computer system and any other entity that processes or stores computer data on behalf of that entity or its users" (sect. 2). While the first part targets ISPs, the second part of the definition is wide enough to cover all internet intermediaries.

Intermediaries are required to cooperate with police officers to provide three types of data; subscriber information, traffic data and content data. These three requirements are considered in detail below.

In cooperating with law enforcement, intermediaries have to balance the need to protect the privacy of their customers who have trusted them with their personal information and communication vis-à-vis their role in the maintenance of law and

order (Kerr & Gilbert, 2004). On one hand, any cooperation efforts by intermediaries will inevitably affect the relationship between the intermediary and its customers. On the other hand, the criminal sanctions imposed for non-compliance do not allow the intermediaries any wiggle room. Legislation imposing such responsibilities on intermediaries must therefore be cognizant of this dynamic and have at its core the dedication to protect and uphold constitutional rights. If legislation does not adhere to the constitutional safeguards, and if intermediaries act according to such legislation, they become complicit in the violation of human rights as they are agents of the state in doing so.[13] They may also be liable for breach of contract and constitutional violations.

Subscriber information

Subscriber information is defined as information disclosing the identity, location and address of a subscriber together with their subscription details (sect. 2). This information is comparable to the details that would normally be available at a telephone directory hence is sensitive (Kerr & Gilbert, 2004). In terms of the 2018 Act, intermediaries will only be required to release this information pursuant to a court order (sect. 50).

Section 50(1) contains a drafting error; as currently drafted, the section suggests that subscriber information may only be obtained for investigation purposes,[14] whereas any other information may be sought for whatever reason.[15] This section needs to be amended so that the rider "is necessary or desirable for purposes of an investigation" covers both section 50(1)(a) and (b).

Traffic data

Traffic data are defined, in section 2 of the Act, as information concerning the origin, destination, route, time, date, size and duration of communication and the type of underlying service. Normally, this would be information such as the sender and recipient of an email, the subject lines of the email and its size, the titles of any attachments, websites visited by a user, and the time spent at each website (Kerr & Gilbert, 2004). This is the footprint of a user's communication on the internet, hence more sensitive and worthy of stricter protection.

The Act anticipates expedited preservation of traffic data as well as real-time collection of traffic data. These are dealt with differently, as we explain below:

Expedited preservation and disclosure of traffic data

For the expedited option, a notice to preserve and disclose traffic data will originate from a police officer or an "authorised person" (sect. 51). The Act is not specific on

13 See *R v Weir* 3d 59 Alta. L.R., 319.
14 Section 50(1)(b).
15 Section 50(1)(a).

who an authorised person will be, or the person's qualifications, save for providing that this will be a person designated by the Cabinet Secretary. The expedited option may only be exercised where there is a risk that the traffic data may be modified, lost, destroyed, or rendered inaccessible. The notice may also require an intermediary to disclose traffic data that would be sufficient to identify the service providers and the path through which the communication was transmitted.

The data specified in the notice are to be preserved for a period not exceeding 30 days. This period may be extended by a court order once the person issuing the first notice shows that the extension is necessary for an ongoing investigation, there is a risk that the data will be lost, and that the cost of preservation of the data for an extended period of time is not overly burdensome (sect. 51(3)).

That a police officer can issue a notice to a service provider to preserve and disclose traffic data without obtaining a court order first is worrisome. Such a provision ignores the safeguards in Article 31(d) of the Constitution of Kenya which protects the privacy of communications. This right is not absolute. However, any limitation thereof has to be in line with Article 24 of the Constitution. Specifically, the extent of the limitation has to be specific. Allowing police officers to bypass judicial approval on the basis of "reasonable grounds" allows the violation of the right to privacy based on a vague and subjective test.

That the court can order the extension of this period to more than 30 days is also of concern. This means that for a period of 30 days or more, the intermediaries ought to preserve every piece of information a user inputs into the internet or downloads therefrom at the intermediary's own cost.

Police officers will also be able to use these orders to identify all the telecommunications providers involved in the transmission of the communication in question.

Real-time collection of traffic data

Real-time collection of data may be done by a police officer, an authorised person as described above or an intermediary. Such collection has to be pursuant to a court order. Intermediaries may collect and record traffic data then submit the same to the police officer. Alternatively, they are obliged to cooperate and assist the police officer to collect and record such information whether the information is transmitted through means owned by the intermediary or not (sect. 52).

Section 52(4) requires that a court order for real-time collection and recording of traffic data ought to allow for the collection to take place for a period not exceeding six months with the possibility of extension by a court order. This will be at the cost of the intermediary.

If an intermediary fails to comply with the obligations under section 52, they may be fined up to ten million Kenyan shillings. Further, a principal officer of the intermediary may be fined up to five million shillings, be imprisoned for up to three years, or be punished by both fine and imprisonment.

Real-time interception of traffic data is a gross violation of privacy. It provides a window into a person's life, revealing not only their particular movements, but also their familial, professional, religious and sexual association and preferences. This measure ought to be used sparingly and only for specified offences (Kerr & Gilbert, 2004).

Interception of content data

Content data have been defined in the Act as the substance, meaning, and purport of a specified communication (sect. 2). In other words, this is the actual text of messages, emails, publications, and search queries. As interception of such communication is a severe violation of the right to privacy, it must only be employed in very special cases.

In terms of the Act, a police officer or an authorised person may apply to the court for an order permitting the police officer or authorised person to collect or record content data in real time. The order may also compel an intermediary to either collect or record the content-data or to cooperate and assist the authorities. Such an order will only apply to specified communication and cannot be for a period exceeding nine months. However, this period may be extended (sect. 53).

Because of the provisions of the Act, it is apparent that intermediaries will have to restructure internally and set up mechanisms to distinguish between traffic data and content data. Instances of cybercrime are on the increase. This will inevitably translate to numerous court orders and notices to cooperate with police officers in the investigation of cybercrimes. It would be prudent for intermediaries operating in Kenya to carry out an audit on how much it will cost to execute the court orders and police notices issued under Part IV of the Act.

International cooperation

International cooperation has become an integral part of combating cybercrime given the transnational nature of crimes committed on or via the Internet (Mittal & Sharma, 2017). While the cyberspace has no borders, police officers have to respect the sovereignty of other countries by collaborating through international conventions or treaties (Mittal & Sharma, 2017, p. 1373). This presents challenges as to the jurisdiction of courts, trans-national investigation, and the use of extra-territorial evidence in cases where this does not exist. Kenya has in place the Mutual Legal Assistance Act, 2001 (Republic of Kenya, 2001). This Act allows Kenya to facilitate the interception of communication, preservation of communication data and covert electronic surveillance at the request of another State.

Part V of the Act is meant to complement the Mutual Legal Assistance Act. Section 58 of the 2018 Act allows the Central Authority created under the Mutual Legal Assistance Act to forward to a foreign state information obtained even where there has been no request for the same. If in the course of an investigation, it is discovered that a service provider in another state was involved in the transmission of communication, the Central Authority will be allowed to disclose the traffic data obtained under Part IV of the 2018 Act to that other state in order to identify the service provider and the path through which the communication was transmitted. With regard to requests to access stored computer data, real-time collection of traffic data, and interception of content data, the Central Authority will be required to obtain the necessary warrants and orders according to the prevailing laws at that time.

6. Constitutionality of the Act challenged

The Act was assented to law on 16 May 2018, and was to come into force on 30 May 2018. However, on 29 May 2018, the Bloggers Association of Kenya (BAKE) obtained court orders suspending the coming into force of the Act, until a petition challenging the constitutionality of the Act is heard and determined.

The challenge focuses on 26 sections in the Act. Part IV of the Act is being challenged. It deals with investigation procedures and requires service providers to provide police officers with subscriber information, traffic data, and content data. According to BAKE, the procedures outlined in Part IV do not meet the threshold prescribed under Article 24 of the Kenyan Constitution. Under the Constitution's Article 24, an Act limiting any fundamental right must clearly state to what extent a particular right is being limited. The limitation should not go so far as to derogate from the core of the right protected by the Constitution. It has been posited by BAKE that the procedure outlined in Part IV is cavalier in its treatment of the right to privacy.

Sections 22, 23 and 24 of the Act have also being challenged, on grounds of limiting the right to freedom of expression.

In our analysis, it is an opportune time for intermediaries with operations in Kenya to join the constitutional petition and challenge the definition of the word "publish", especially in section 24, in order to avert strict liability of intermediaries.

7. Conclusions and recommendations

The position proffered by the 2018 Act in section 56 is that intermediaries will not be liable for merely providing a service. Criminal liability will only be imposed if the intermediary had actual knowledge or notice, or if the intermediary acted out of wilful malicious intent. The foundation of such a statement on liability is noble, as it seeks to protect the internet infrastructure while punishing bad actors. However, the

test that is created is alarmingly subjective, leaving it to the courts to determine as and when liability will attach.

There are also other sections, such as sections 22, 23 and 24, which hint at intermediary liability and appear to be in conflict with the general statement on liability in section 56. These contradictions will be left to the courts for interpretation. Judicial discretion often causes uncertainty on the issue of intermediary liability, and is hence undesirable.

Where intermediaries would be hardest hit, however, is by the requirement for their cooperation in investigation procedures. The Act essentially converts intermediaries into state agents, with the added threat of criminal liability should they not offer their assistance as required. In addition, the Act potentially opens a floodgate of opportunities for law enforcement to turn to intermediaries for assistance, yet remains silent on the cost of such cooperation.

That constitutionality of the Act is now in challenge means that there is a possibility that some of the sections will be expunged from the Act should they be found to be non-conforming to the Constitution of Kenya. Any conclusion on intermediary liability in this article is therefore subject to the court's finding.

We now provide our recommendations for subsequent amendment of the Act.

Preliminary definitions
The following terms are used in the body of the Act but are never defined in the preliminary page: public security, public health, access, unauthorised, protected computer system, critical data/database, national information infrastructure, and illegal devices. It is proposed that, for the avoidance of ambiguity, appropriate definitions for the same are provided.

Content offences
Sections 22 and 23: False publications and publication of false information: These two sections prescribe offences in a manner that amounts to an unconstitutional limitation of freedom of expression. Failing to describe what activities amount to "publish" also puts intermediaries at risk.

- *Proposal 1: Publication of false information should only be an offence if it amounts to hate speech, propaganda for war or any of the exceptions listed in Article 33(2) and (3) of the Constitution.*
- *Proposal 2: Define what amounts to a publication. It is proposed that the offence be defined to only capture the source of the publication to avoid netting innocent internet users who only share the information.*

Section 24: Child pornography: The definition of "publish" in section 24 may be prejudicial to intermediaries as it introduces a strict liability regime despite the conditional liability position taken by section 56(2). The word "publish" includes "making available in any way". Further, intermediaries offering cloud storage solutions may be found guilty of possession of child pornography.

- *Proposal 1: Redefine the offence of child pornography. Specifically remove the definition of publish that denotes 'making available in any way'.*
- *Proposal 2: The offence of possession of pornographic material should be restricted to primary offenders to protect intermediaries who offer cloud storage facilities.*
- *Proposal 3: Section 24 ought to be harmonised with Section 16 of the Sexual Offences Act, particularly with regard to the amount of fines payable and duration of sentences.*
- *Proposal 4: The lawful possession of child pornography should only be limited to law enforcement purposes. Even in this case, there should be clear provision for what the lawful management of child pornography in the course of law enforcement entails and by whom.*

Intermediary liability

Various sections in the Act touching on intermediary liability require harmonisation.

Section 56: Confidentiality and limitation of liability: Section 56(2) attempts to create a safe harbour for intermediaries. However, the general language used in the Act leaves room for manipulation. For instance, a bulletproof hosting service that offers "hacking-as-a-service" may rely on this section to avoid liability since availing a service exempts it from liability under section 56(2).

- *Proposal 1: Enumerate safe harbours for intermediaries based on function, e.g., conduits, caching, hosting and information location. Anything outside these harbours attracts liability.*

Section 56 also imposes liability on intermediaries in cases where there is actual knowledge and notice of an offence. Some aspects of this section need clarification.

- *Proposal 2: What constitutes adequate knowledge and notice needs to be defined. Proof of knowledge and notice must also be determinable. For instance, the Act could impose a duty on intermediaries to designate a reporting officer. Once a complaint is sent to the reporting officer, this amounts to actual knowledge and notice.*
- *Proposal 3: Enumerate what an intermediary is to do once it is notified of an offence, e.g., disable access or discontinue service, report to the authorities or send a cease notice. Failure to take any such action is what ought to constitute an offence, not mere knowledge.*

The approach taken by the Act is to impose criminal liability to secure co-operation by intermediaries. The threat of criminal responsibility on the intermediaries themselves may lead to overzealous censorship.

- *Proposal 4: We propose a change of approach from conditional liability to broad immunity. The Act could set out a requirement for intermediaries to come up with content policies on areas such as child pornography and hate speech. These policies ought to meet a certain threshold. Failure to abide by these policies must lead to loss of service. The intermediary should be further protected from liability for discontinuing service based on their internal policy. This approach would achieve intermediary co-operation without the unnecessary hostility.*

Investigation procedures

Sections 47-56: These sections provide for investigation procedures including search and seizure of stored computer data, record of and access to seized data, production order and grounds for such application of a production order by a police officer, expedited preservation and partial disclosure of traffic data, the period for such preservation and extension of the said period. These sections have the highest impact on Intermediaries and we propose the following as mitigating measures.

- *Proposal 1: Warrants for obtaining digital evidence should be approached differently from traditional warrants. To obtain them, a police officer must not only be able to identify the premises to be searched but also the computer system to be searched. The wording of the warrants should reflect realities in the digital age e.g. cloud storage.*
- *Proposal 2: Where computer systems are seized as part of an investigation, they should be returned within a specified period of time. This will not only encourage speed on the part of police officers but will also ease the burden on the owner of systems.*
- *Proposal 3: The owner of a computer system must be allowed to access a seized system and copy it to avoid jeopardizing their trade.*
- *Proposal 4: The circumstances that warrant a police notice to record and disclose traffic data without a court order must be specifically and explicitly defined by legislation to avoid abuse of power.*
- *Proposal 5: Investigation should be restricted to police officers and authorised government agencies and experts. Co-opting private industry players as state agents is open to abuse, particularly if the co-opted investigator is from a rival company and able to exploit intellectual property encountered during investigations.*
- *Proposal 6: The requirement that intermediaries cannot disclose details of any warrant or production order should be time bound. Once the investigation is complete, intermediaries should be given the option to disclose the level of their co-operation to their respective clients. This enhances the client-intermediary trust relationships and is in line with international best practice.*
- *Proposal 7: Expedited preservation of traffic data should be court ordered. Leaving this to the police officers may lead to a multiplicity of notices, which may translate to higher costs on the part of the intermediary.*
- *Proposal 8: Real-time collection of traffic data should be reserved for specific offences or circumstances.*

- *Proposal 9: The cost of monitoring, collecting, preserving and producing data should be borne by the State and not by the intermediaries.*
- *Proposal 10: Section 50 should be amended to include the rider 'is necessary or desirable for purposes of an investigation'. This would qualify and cover the intentions of both sections 50(1)(a) and (b).*

References

Article 19. (2013). *Internet intermediaries: Dilemma of liability*. Retrieved from https://www.article19.org/wp-content/uploads/2018/02/Intermediaries_ENGLISH.pdf

Best, M. L. (2004). Can the internet be a human right? *Human Rights & Human Welfare, 4*(1), 22–31.

Business Daily. (2018, April 6). Two men charged with hacking into Safaricom system. Retrieved from https://www.businessdailyafrica.com/corporate/Two-men-charged-with-hacking-Safaricom-system/539550-3880240-140vv0az/index.html

Cheeseman, N. (2008). The Kenyan elections of 2007: An introduction. *Journal of Eastern African Studies*, *2*(2), 166–184. https://doi.org/10.1080/17531050802058286

Communications Authority of Kenya (CAK). (2017). *First quarter sector statistics report for the financial year 2017/2018 (July-September 2017)*. Retrieved from http://www.ca.go.ke/index.php/statistics

Council of Europe (2001). Convention on Cybercrime (Budapest Convention).

Dinwoodie, G. B. (Ed.). (2017). *Secondary liability of internet service providers*. Springer. https://doi.org/10.1007/978-3-319-55030-5

Englander, E., Donnerstein, E., Kowalski, R., Lin, C. A., & Parti, K. (2017). Defining cyberbullying. *Pediatrics, 140(Supplement 2)*, S148–S151. doi:10.1542/peds.2016-1758u

George Andare v the Attorney General & 2 Others [2016] eKLR, High Court of Kenya.

Gürkaynak, G., Yılmaz, İ., & Durlu, D. (2013). Understanding search engines: A legal perspective on liability in the Internet law vista. *Computer Law & Security Review, 29*(1), 40–47. https://doi.org/10.1016/j.clsr.2012.11.009

Hornik, J., & Villa llera, C. (2017). *An economic analysis of liability of hosting services: Uncertainty and incentives online*. Bruges European Economic Research Papers 37/2017.

International Telecommunication Union (ITU). (2017) *Global cybersecurity index.* Geneva.

Kerr, I. R., & Gilbert, D., (2004). The role of ISPs in the investigation of cybercrime. In T. Mendina, & J. L. Britz (Eds.) (2004), *Information ethics in an electronic age: Current issues in Africa and the world* (pp. 163–172). Jefferson, NC: McFarland and Company.

Kerr, O. S. (2005). Search warrants in an era of digital evidence. *Mississippi Law Journal, 75*(1), 85–145.

Kreimer, S. F. (2006). Censorship by proxy: The First Amendment, internet intermediaries, and the problem of the weakest link. *University of Pennsylvania Law Review, 155*(1), 11–101. https://doi.org/10.2307/40041302

Kurbalija, J. (2016). *An introduction to internet governance*. Switzerland: Diplo Foundation.

MacKinnon, R., Hickok, E., Bar, A., & Lim, H. I. (2015). *Fostering freedom online: The role of internet intermediaries*. Paris: UNESCO.

Mittal, I. P. S., & Sharma, P. (2017). A review of international legal framework to combat cybercrime. *International Journal of Advanced Research in Computer Science*, *8*(5), 1372–1374. https://doi.org/10.2139/ssrn.2978744

Ndemo, B., & Weiss, T. (Eds.) (2016). *Digital Kenya: An entrepreneurial revolution in the making*. Springer.

Perset, K. (2010). *The economic and social role of internet intermediaries.* Paris: OECD. https://doi.org/10.1787/5kmh79zzs8vb-en

Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). *Anonymity, privacy, and security online*. Washington, DC: Pew Research Center.

Republic of Kenya. (1963). Evidence Act, 1963.

Republic of Kenya. (1998a). Kenya Communications Act, 1998.

Republic of Kenya. (1998b). Kenya Information and Communications Act (KICA), 1998.

Republic of Kenya. (2001). Mutual Legal Assistance Act, 2001.

Republic of Kenya. (2006). Sexual Offences Act, 2006.

Republic of Kenya. (2008a). Kenya Information and Communications Act, 2008. Retrieved from http://www.ca.go.ke/index.php/sector-legislation

Republic of Kenya. (2008b). National Cohesion and Integration Act, 2008. Retrieved from http://www.kenyalaw.org/lex/actview.xql?actid=No.%2012%20of%202008

Republic of Kenya. (2010). Constitution of Kenya, 2010. Retrieved from http://kenyalaw.org/kl/index.php?id=398

Republic of Kenya. (2013). Kenya Information and Communications (Amendment) Act, 2013. Retrieved from http://www.ca.go.ke/index.php/sector-legislation

Republic of Kenya. (2018). Computer Misuse and Cybercrimes Act, 2018. Retrieved from http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

Serianu, K. (2017). *Cybersecurity report 2017: Demystifying Africa's cyber security poverty line.* Retrieved from http://www.serianu.com/resources.html

Sloot, B. (2015). Welcome to the jungle: The liability of internet intermediaries for privacy violations in Europe. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *6*(3), 211–228.

Technology Coalition. (2015). *Employee resilience guidebook for handling sexual exploitation images*. Retrieved from http://www.technologycoalition.org/wp-content/uploads/2015/01/TechnologyCoalitionEmployeeResilienceGuidebookV2January2015.pdf

Truyens, M., & Van Eecke, P. (2016). Liability of domain name registries: Don't shoot the messenger. *Computer Law & Security Review, 32*(2), 327–344. https://doi.org/10.1016/j.clsr.2015.12.018