CYBER SECURITY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Body** | **Regulation** | **Comments/Proposals** | **Justification** | **Authority’s response** |
| **Safaricom** | **R. 5 Computerized Non Data Breaches** | a) intercept or attempt to intercept computerized data fraudulently by technical means during non-public transmission to, from or within a computer system;  b) intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether  or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches;  (c)even through negligence, process or have personal data processed without complying with the preliminary formalities for the processing.  **Proposal**  (b) intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal or *commercial purposes* as if it  were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches;  (e)even through negligence, process or have personal data processed without complying with the preliminary formalities for the processing. | Non-public transmission used within this context is not clear from the Regulations. We therefore kindly request further clarity from the Authority  We kindly propose the addition of the word commercial purposes to the Regulations since commercial considerations are also a motivating  factors towards alteration of such data |  |
|  | **R. 7 Operation and use of Cyber Cafes and Public Wireless Hotspots** | Operators of Cyber Cafes and Public Wireless Hotspots shall:  a) identify users before providing them with services;  b) provide a system for user registration which ties each user to a mobile phone number. Operators of cyber cafes and public wireless hotspots shall be required to inform users of their service that it is illegal to use an unregistered mobile phone number for registration and access to cyber cafe and public wireless hotspot services;  c) Information collected in (b) shall be made available to the authority for further action, as and when is deemed necessary.  d) maintain a register for all its clients;  e) install Closed Circuit Television (CCTV) cameras to record the identify of its clients;  f) use Public Internet Protocol (IP) addresses for its computers;  g) ensure that system logs are retained in their original for periods of not  less than one (1) year from the date of the communication. The Authority may issue guidelines on retention of communication logs from time to time.  h) required to report any cyber-crime incidents to the Authority within 24-hours and as may be prescribed by the Authority from time to time;  i) required to obtain an authorization from the Authority to provide cyber-café and public wireless hotspot services;  j) submit compliance returns to the Authority as may be prescribed from time to time.    Kindly delete and amend this Regulation as follows:  *Operators of Cyber Cafes and Public Wireless Hotspots shall:*  *a) ……………………;*  *b) Provide a system for user registration, which will include details of the User’s valid mobile phone number. Operators of cyber cafes and public wireless hotspots shall be required to inform users of their service that it is illegal to use an unregistered mobile phone number for registration and access to cyber cafe and public wireless hotspot services;*  *c) ……………..*  *d) maintain a register for all its clients in the case of a Cybercafe ;*  *e) ………………..;*  *f) ………………..;*  *g) ………………...*  *h) required to report any cyber-crime incidents to the Authority within 24-hours of discoveryand as may*  *be prescribed by the Authority from time to time required to obtain an authorization from the Authority to provide cyber-café and public wireless hotspot services,*  *i) …………………*  *j) maintain softwares for the monitoring and prevention of malicious programmes and viruses within Cybercafes*  *submit compliance returns to the Authority as may be prescribed from time to time.* | Safaricom appreciates the need to ensure all subscribers accessing Public Wifi Hotspots are registered for purposes of security surveillance. We therefore propose to clarify this Regulation to state that part of the registration requirements for a user of the service will be to submit a valid mobile phone number.  With respect to Regulation 7 (h) we propose to add the words *of discovery* to provide further clarity on when cases of cybersecurity attacks should be escalated.  Further, Cyber cafes, have numerous cases of keyloggers in both hardware and software. Keyloggers are software programs or hardware devices used to capture keystrokes or credentials for purposes of committing fraud. Cyber Cafes should therefore have the responsibility to regularly check for hardware keyloggers and scan for software keyloggers using robust anti-viruses in order to protect consumers of their services from such attacks. |  |
|  | **R. 11 Categories of Data to be retained** | d) data necessary to identify the type of communication:  i. ……………  ii. concerning Internet e-mail and Internet telephony: the Internet service used;  Kindly amend this Regulation as follows:  *i………*  *ii. Where possible, concerning Internet e-mail and Internet telephony: the Internet service used;* | Please note that this section will not necessarily apply to telecommunications operators given that we offer platforms for OTT services and thus impractical to provide the level of detail requested with respect to such services. |  |
|  | **R.14 Framework for Reporting, Investigating, Prosecuting and Managing Cybercrime** | (a) All licensees shall be required to report any cyber-crime incidents to the National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC), a function of the Authority, within 24-hours and as may be prescribed by the Authority from time to time;  (b)……….  (c) The Authority shall require service providers to-  (i) inform the authorized agencies of alleged illegal activities under-taken, or information provided, by recipients of their service;  (ii) communicate to the Authority and any other authorized agencies, at their request, information enabling the identification of recipients of their service; and  (iii) provide access to telecommunication systems for purposes of investigating and prosecuting cyber-crime offenses  Proposed Amendment  *a) All licensees shall be required to report any cyber-crime incidents to the National Kenya Computer Incident Response Team – Coordination Centre (KE-CIRT/CC), a function of the Authority, within 24-hours of discovery and as may be prescribed by the Authority from time to time*  c) Please delete this provision | We kindly request the addition of the words *of discovery* to provide further clarity on when cases of cybersecurity attacks should be reported.  Further, we propose the deletion of Regulation 14 (c) for the reason that the access to information mandated under this Regulation would contravene provisions already existing in Security related legislations (NIS Act, POTA) . These legislation already have a process in place for purposes of law enforcement include inter alia providing a court order or warrant prior to accessing such information. Further, it would be impractical to mandate Operators to undertake proactive disclosures of such incidences because to do so would require interception of telecommunications services which is prohibited under the KICA. Therefore compliance with such a provision would place Operators in great jeopardy. |  |
| **KCB** | 5  6  13(d)  14(a)  5 | Define “preliminary formalities” for clarity    Amend the section on content related offences so as to take observation into consideration  Delete the provision on data protection and data security  Amend 'cyber-crime incident' to read ‘reasonable suspicion that a cyber-crime has been/is being committed’  Amend ‘alleged’ to read ‘suspected illegal’ | For website/webpage owners, it should be a defence that the offending material was posted by a website user (not being the website/webpage owner) and/or that the material was taken down within a reasonable time after receipt of notice that the material is offensive. This is because material posted particularly on social networking/blogging pages is, for the most part, beyond the page owner's control  A service provider should be allowed to retain data at its discretion. Data should be retained so long as consent was provided and data security requirements are complied with.  A 'cyber-crime incident' should be defined as a reasonable suspicion that a cyber-crime has been/is being committed. This is because only a court (as opposed to a licensee) can determine whether a cyber-crime has been committed. Otherwise, if an incident is reported and ultimately found not to have been a cyber-crime, it would be unfair for a licensee to be held liable for providing false information to the authorities.  This should refer to reasonably suspected illegal activities/information provided |  |
| **Liquid Telecom** | Definitions  Objectives  Section 4 | Section on electronic commerce has been repeated in the electronic transactions regulations  Definitions existing in the Act have been replicated in the Regulations.  Inconsistency of definitions  Foreign definitions  Inappropriate to set out objectives for the regulations. Should be deleted.  Subordinate cannot create criminal offences.  Has been lifted from the AU convention on cyber security.  These provisions also already exist in our KICA specifically s. 83U, 83X and 84B of the Act.  Specifically, Section 4 a) of the Cybersecurity Regulations is largely covered by Section 83U of the Act, Section 4 b) and Section 4 c) are not well covered and would be best dealt with as an amendment to the Act, Section 4 d) is covered by Section 83W (1)(b) and Section 83X(2) of the Act, Section 4 e) is covered by Section 84B of the Act and Section 4 f) is already covered by 83X(1) of the Act. | Appears to be an error.  Definitions that exist in legislation should not reappear in subordinate legislation  Definitions should be aligned to Kenyan context  This is not primary legislation and as such should not include an objective  Only primary legislation can do so  This duplication could result in confusion and prosecutions being overturned due to this uncertainty and a lack of due process. Accordingly Liquid Telecom submits that this section should be reconsidered in its entirety. |  |
|  | Section 5 | Liquid Telecom notes that this is a direct copy of Article 29 1 of the African Union Convention on Cyber Security and Personal Data Protection.  The Act already contains in essence, the provisions set out in the Cybersecurity Regulations and Liquid Telecom notes that this section in essence repeats Sections 32, 83W – 83X and 84B of the Act.  To the extent that CAK is of the view that Sections 32, 83W – 83X and 84B of the Act need to be amended to include some of the items contained in the Cybersecurity Regulations, then it is the Act that should be amended and such amendment cannot be introduced “behind the scenes” through regulation.  Liquid Telecom notes that Regulation 5 e) and f) as set out above are not covered by the Act, but instead relate to data privacy, which is not covered by the Act at all. | Accordingly the inclusion of these provisions in regulations will be ultra vires the Act. In addition, by aligning the Cybersecurity Regulations to the African Union Convention on Cyber Security and Personal Data Protection, the Cybersecurity Regulations have introduced concepts that are not relevant at all.  This duplication could result in confusion and prosecutions being overturned due to a lack of due process. Accordingly Liquid Telecom submits that this section should be reconsidered in its entirety. |  |
|  |  | Liquid Telecom notes that this section is a direct copy of Article 29 1 of the African Union Convention on Cyber Security and Personal Data Protection.  The Laws of Kenya already contain, in essence, the provisions set out in the Cybersecurity Regulations and  Liquid Telecom notes that this section in essence repeats Sections 11 and 16 of the Sexual Offences Act (CAP 62A), various provisions of the Films and Stage Plays Act (CAP 222), various provisions of The Penal Code (specifically Sections 96 and 77), the National Cohesion and Integration Act, 2008 (specifically Sections 13 and 62) and the Media Act No. 3 of 2007 (specifically the Second Schedule to the Act, titled “Code of Conduct for the Practice of Journalism in Kenya”, Regulation 25).  Liquid Telecom notes that the Cybersecurity Regulations has made reference to a “computer system” in respect of each of these offences. Liquid Telecom submits that the most appropriate way of achieving this equivalence (to the extent that it does not already exist, which Liquid Telecom doubts) is to provide a single revision to the Act (possibly at Section 83G) indicating that there is equivalence not just for the purposes of records but also for the purposes of all offenses. | Liquid Telecom submits that such extension to computer systems cannot and should not be introduced “behind the scenes” through regulation. This attempt runs the risk of creating two “layers” of crime: for example distribution of child pornography through a physical medium (such as a disk or printed photographs) and by way of a computer system. That then creates two paths for criminal prosecution, different sentences and burdens of proof.  This duplication could result in confusion and prosecutions being overturned due to a lack of due process. Accordingly Liquid Telecom submits that this section should be reconsidered in its entirety. |  |
|  |  | Cyber cafes provide an essential service in enabling the digital economy, and we believe that onerous regulations to over complicate them and over regulate will have a deeply damaging effect on the digital growth of Kenya.  Wi-FI spots:   * The majority of these hotspots are not truly “public” in that they are contained within a specific location, such as a hotel, a shopping mall, a school or university; * It is very seldom that the owner of the premises is actually the operator of the hotspot; and * The operation of the hotspot is generally an adjunct to the business of the owner / operator of the premises. It is inconceivable that a hotel operator can be said to be a telecommunications operator.   Internet cafes:   * These establishments generally do not operate a telecommunications system, but rather allow a member of the public to access a telecommunications system operated by a licensed operator, for a fee; and * The Act does not contain a specific definition of customer premises equipment (CPE), however the generally accepted approach globally is that there is no licence required beyond the customer demarcation point (fixed or wireless) and that CPE is type approved, but the use thereof is not regulated.   In attempting to introduce a licensing requirement (regulation 7 i)) Liquid Telecom submits that the CAK has overstepped its boundaries and is attempting to enter the realms of legislation. Liquid Telecom submits that any attempt to introduce such a dramatic change should be by way of legislative intervention and not through subordinate legislation.  In respect of the definition of “cyber café“ Liquid Telecom submits that this definition is overly broad and would include every school, college and university. In addition, if an operator were to bundle equipment (a mobile device or a fixed computer) with an Internet access service against payment of a monthly fee (without outright purchase) then that operator could become a cyber café. Liquid Telecom submits that further thought needs to go into this definition, specifically in the light of a clear understanding of the problem that the Cybersecurity Regulations seek to address.  In respect of the definition of “public Wi-Fi hotspot” (also referred in the body of the Cybersecurity Regulations as “Public Wireless Hotspots”), Liquid Telecom submits that the reference to “site” is confusing. We are uncertain if it is the site that triggers the compliance function or the network? For example, if a single operator provider Wi-Fi access at ten hotels, is that one network or ten? In addition, the public distinction is likewise not clear: does restricting the network to hotel guests make the network public or private? Similarly with employees, guests, members of the public, students?  Is the intervention proportional to the effort being imposed on the so-called “operators”. In the absence of any clear motivation for these requirements, Liquid Telecom submits that the obligations are not proportionate.  The regulations are unclear for example: how does an “operator” identify a user, if the user attempts to connect via Wi-Fi? It is a device that attempts to connect and not a specific person. Does that imply that a potential user must present him or herself and identify him or herself physically? | There is concern about the arbitrary nature of the obligations: information must be made available “as and when deemed necessary” and without any clear or justifiable reason. There is no limitation on the retention of identification data. |  |
|  |  | Technical concerns  • How does the operator tie a user to a mobile phone number? What is to stop a potential user giving a third party’s number? Does an operator need to have access to the mobile phone number database to perform verification?  • How exactly does installing CCTV cameras serve to record the identity (we presume identify should be identity here) of clients? Does it mean there must be a CCTV camera in every room of a hotel if the hotel offers Wi-Fi? How does an operator ensure complete coverage of its premises? For how long and in what format must those images be retained? Does an operator have an obligation to verify the recordings to ensure that the person can be identified?  • The use of public IP addresses does not make any sense with regards Wi-Fi hotspots. It may make some sense with regards Internet cafés, however the Internet café will be reliant of it s service provider for the allocation of the IP ranges, as no Internet café has the resources to acquire a public range directly from the regional Internet registry, in this case AfriNIC. |  |  |
|  | Regulation 8 - Management of critical internet (sic) resources   1. Liquid Telecom notes that the convention, when referring to the network of interconnect networks which use the Internet protocol, known as “the Internet”, the convention is to capitalise the letter “i” indicating it is a proper noun and the single interoperable Internet. Liquid Telecom suggests that this convention be adopted throughput the Cybersecurity Regulations. 2. Liquid Telecom notes that the term “critical Internet resources” (also sometimes “critical Internet infrastructure”) is often used but does not have a single definition. The ITU has noted that has not been explicitly defined in ITU’s Basic Text or decisions made by ITU bodies. However, many references to the protection of critical national infrastructure exist especially in the context of security of telecommunications/ICT networks and services. Liquid Telecom suggests that the term “critical Internet resources” is an evolving term, the meaning of which is dependant on current circumstances and will evolve over time (in this regard, Liquid Telecom refers the CAK to Geoff Houston’s article On the Hunt for "Critical Internet Resources" at http://www.circleid.com/posts/critical\_internet\_resources/). | Accordingly Liquid Telecom suggests that the term “critical Internet resources” is suitable only for a policy document. However legislation must be specific and subordinate legislation such as the Cybersecurity Regulations even more so. The Cybersecurity Regulations must be precise in terms of the matters being regulated, or they risk being ultra vires the Act. Liquid Telecom submits that the definition and Regulation 8 are so vague so as to not to meet the threshold for lawfulness. |  |
|  |  | Regulations 11 – 13 – Data retention  This regulation has been copied from the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.  This is disturbing, as the sections copied have been taken out of context and the regulation contains none of the protections that are contained in the Directive, but all of the obligations of “service providers”. Furthermore, this ignores the fact that the Directive has been declared invalid by the European Court (Grand Chamber) as of 8 April 2014 in the matter of Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others.  In addition, the definition of Service Provider is incredibly broad and bear no resemblance to the obligations in the Directive referenced, This definition would include every parent who allows a child to access the Internet from home, every school, college or university, every employer who provides access at work, as well as licensed operators. Liquid Telecom submits that there is no legislative authority under which this regulation may be imposed on any party, neither operator nor other party.  The only legislative authority for the provision of data is Section 27(2)(d) of the Act which provides for regulations concerning: the period during which and conditions subject to which messages and papers relating to telecommunication services belonging to, or in the custody of telecommunication operators shall be preserved;”  There is nothing in Section 27(2)(d) which allows for the indiscriminate obligation to store data.  In this regard Liquid Telecom notes that where other legislative regimes require data collection, it is done in terms of generally adopted standards, such as global lawful intercept (LI) requirements and standards developed by the European Telecommunications Standards Institute (ETSI), 3rd Generation Partnership Project (3GPP), or CableLabs organisations. The fluid and unstructured obligations set out in regulation 8 are not capable of compliance as they are not anchored in any known or defined standard. | Liquid Telecom rejects any attempt to introduce data retention requirements without a clear legislative function, clarity on the cost (in many countries the state bears the cost of data retention) and the technical standard applicable |  |
|  | 14 | Framework for Reporting, Investigating, Prosecuting and Managing Cybercrime  Liquid Telecom notes the provisions of regulation 14 and appreciates the intent of this regulation. However Liquid Telecom is concerned that it is contradictory and does not allow for a collaborative working relationship between the CAK and licensees.  Specifically, Liquid Telecom notes that regulation 14(b) is entirely appropriate and supported by Liquid Telecom, however the contradiction with the obligations in 14 (c) are stark and Liquid Telecom is unable to resolve the contradiction. In particular the obligation to “provide access” is unacceptable. Liquid Telecom is willing to provide evidence as may be required for a prosecution, in terms of the Penal Code, but will not open its systems up to the CAK or any other party.  Liquid Telecom welcomes the notion of a collaborative framework (at 14 (e)) and submits that this is more likely to achieve results than a heavy-handed approach.  Liquid Telecom thanks CAK for the opportunity to make this submission and will make itself available to provide CAK with further information, should this be required. |  |  |
| **Microsoft** |  | Definitions and offences  We recommend narrowing the following definitions:  **Computer system**: while this definition does not appear intrinsically problematic, we note that it fails to include a reference to ‘automatic processing of data’, which is a key component of the definition of computer systems in the Cybercrime Convention.  **Computerized data breaches**: In the section dealing with “computerized data breaches, Microsoft would like to see several clarifications, in particular around point f) which refers to the “Convention” without clarifying which convention it is referring to. Moreover, we would like to see further clarification to whom a “party” under point b) refers to, as it is currently left undefined. Finally, we would recommend that criminal liability is attached to negligence only for repeat offenders in cases of gross negligence.  **Critical internet resources**: Microsoft would recommend the government specify what it means with “critical internet resources” precisely, by providing a definition of “vital infrastructure” in the text of the Regulation. The definition as it stands at the moment does not make it clear whether the resources referred to represent critical information infrastructure or resources typically referred to as such within the scope of internet governance. From our perspective, it is vital to keep the notion of criticality as narrow and focused as possible. The EU Network and Information Security (NIS) Directive, for example, has limited the approach to “critical internet infrastructures” to Internet Exchange Points (IXPs), top-level domain name service providers and domain name system service providers.  **Disruption:** Microsoft would also recommend omitting the definition of “disruption” and replacing it with a definition of “incident”, which is an established term in cybersecurity law internationally. For example, the NIS Directive of the European Union defines incident as “incident" means any circumstance or event having an actual adverse effect on security.”  **Interception:** Microsoft also recommends that the definition of the “interception” is aligned more closely with the definition of “illegal interception”, as put forward in Article 3 of the Budapest Convention on Cybercrime. In particular, the definition of interception – and similar for those of other offences defined in the draft law – need to include a reference to “dishonest intent.” Only if these offences are committed with “dishonest intent” should the activity be considered under criminal law. Otherwise, many “white hatted” computer security researchers who engage in similar behavior but have no intent for wrong-doing, might be inadvertently captured within the scope of this law. This would have significant adverse effects on computer security research in Kenya and beyond.  Building on this, we propose that for those offences dealing with malware, passwords, and other security information, it is essential that Kenyan cybersecurity/cybercrime legislation provide for exemptions that enable security researchers to continue to identify threats, anomalies, and vulnerabilities and then share tools, mitigations, code, technologies, and other processes that may help protect those machines. Moreover, most of information technology is considered “dual use.” We would therefore urge against persecuting individuals or entities automatically, solely based on their possession of such technology.  **Licensee:** Microsoft recommends a definition of “licensee” is included in the Regulation to clarify which of the categories, as outlined under the Unified Licensing Framework is referred to here: e.g. network facilities provider, application service provider or content service provider.  **Offences:** As mentioned above, we recommend that the section of the Regulation dealing with offences should be rephrased to criminalize the unauthorized access to computer data by infringing security measures with intent to obtain computer data without a right or other dishonest intent. In addition, fraudulent activity is referred to several times in this section. We would encourage the Kenyan government to ensure consistency with existing laws covering this type of criminal conduct offline so as to avoid unnecessary duplication  **Service provider:** Microsoft recommends that the definition of ‘service provider’ should be consistent with the equivalent definition contained in the Cybercrime Convention. | Microsoft supports the decision to keep the definitions close to those included in the Budapest Convention on Cybercrime and would recommend the government goes even further in aligning to it. A harmonized approach, would amongst other things, ensure smoother international cooperation in this space, which is one of the stated objectives of the government. |  |
|  |  | Microsoft expresses concerns with the requirement to report any offences to the Cybercrime centre within 24 hours. States that it is impractical.  Proposal – operators should be required to “report incidents with a significant impact within a reasonable timeframe after having become aware of them  Define – “significant impact” and the parameters for establishing such significance. Emergency situations could fall as exceptions to this reporting obligation  Government should consider and lay out the implementation and management of the framework needed, as well as consult with the private sector to ensure viability of its implementation.  Technical capabilities to adequately transmit, manage, store, and safeguard incident-related date and clearly identified authorities or procedures for reporting need to be put in place. It is also important that particular care is taken when it comes to ensuring privacy and data protection in such instances, and that the program does not expose the providers sharing the information to any liability for their actions  It is important that if as a last resort reporting is put in place it should track models contemplated in European and US law, and not create an excessive and overbroad reporting regime. | The timeline is too short as the victim may not even be aware that the crime is occurring  Operators should first and foremost be enabled to deal with emergencies, then report facts to the authorities afterwards.  Failure to have an understanding of the problems being solved could result in generation of lots of data and distract security operations from significant threats. |  |
|  |  | Against the proposal that all public information is hosted in Kenya.  Instead of a blanket ban of having any public information hosted outside of Kenya’s borders, a more nuanced approach should be employed which centers on effective classification of data.  The section on promotion of local content should be omitted from this particular Regulation. | Such an approach would severely limit the government ability to utilize the full power of cloud computing in provision of e-government services.  Through data classification, the Government of Kenya can identify its most critical/classified data and ensure that only such critical data be hosted within Kenya. Broadening the category of critical data to include a wide range of public information would severely limit the government’s ability to use, move, store, and secure information under commercially reasonable and user-friendly approaches. A good example of such a framework can be found in the UK government where it was found that that 90% of all government data was not classified and therefore not of critical business impact.  The Regulation should focus solely on achieving cybersecurity across the critical online infrastructure. |  |
|  |  | Section on Electronic commerce should be in the electronic transactions regulations. |  |  |
| **K&O** |  | Regulation 7 –  Provide clarity on basis of identification.  How will a cyber café or wi fi operator maintain a register of clients most of whom are walk in first time clientele who may never return?  Eliminate the requirement for CCTVs in cyber cafes.  The proposed measures to address insecurity over Wi-Fi in our view is not the best way to address this insecurity, since there are many more technical/technological methods to address the issue of security over networks.  Regulation 15: Why does the CA feel the need to spell out in great detail the issues of jurisdictional reach in these subsidiary regulations when it is clear in the primary legislation (KICA) the role of the CA. Further there are other more appropriate pieces of legislation that address the issues of jurisdiction. | It is not clear on what basis this identification will be done and whether it will be vide and ID or other means of identification.  This is impractical.  Costly to the average cyber café owner, and will create a regulatory obstacle which will increase cost of doing business and act as a barrier to entry  It is possible that even with the proposed measures to address Wi-Fi users Wi-Fi which passes through walls/ extends out of buildings can be easily hacked by persons who are not duly registered as proposed in the draft regulations. |  |
| **Moses Karanja (CIPIT)** | 7(a) | Proposal that this regulation reads as follows -  “Any information of any user collected by a cyber café under this rule shall be collected, handled, stored and disclosed in accordance with the personal data processing regulations for a period not exceeding twelve months from the date of collection of that information.” | This clause requires identity disclosure of Internet users but it remains unclear how this will be verified and how confidentiality of collected personal information will be maintained. |  |
|  | 7(b) | The threat modelling by the regulator on this clause misses the technical option of changing  The device MAC address or IMEI spoofing.  A criminal seeking to use a network will more likely than not hide their device and IP address.  On a Mac OSX terminal, for example,  `ifconfig <interface> link <new\_mac\_address>`  Will change the MAC address for <interface> to the value  <new\_mac\_address> if you have administrator access.) | In terms of meeting the stated objective of “…developing a framework for facilitating the investigation and prosecution of cybercrime offences.”, the requirement exposes private data for an end that is technically easy to circumvent. |  |
|  | 7 (c) | Information collected as per this regulation should be availed to a third party after a judicial order has been issued to that effect.  **Proposed Amendment:**  At a minimum, “Information collected in (b) shall be made available to the authority for further action, up on production of a judicial order, as and when is deemed necessary.” At best, Avoid collecting of mass data of all Internet users and rather focus on targeted individuals with authorization from the judiciary. |  |  |
|  | 7(d) | Delete this clause on the requirement for a register of all clients to be maintained | This regulation is quite ambitious since clients to Wi-Fi hotspots, coffee joints and cyber cafes are patronizing these places and may never come back again. The extra step of registering internet users is time consuming in practical sense and might easily be ignored by businesses whose sole aim is not internet service provision (Internet is a complimentary service) |  |
|  | 7(e) | Suggests that this clause be deleted. Preferably. | CCTV technology deployed in public Internet spots and cyber cafes poses the question of whether the benefits outweigh the costs (both financial and social). Indiscriminate surveillance exerts fear on innocent citizens forcing them to change behaviour in public to avoid ‘attracting attention’ from the cameras and the eyes behind them. This however does not deter criminals who may even appreciate such recordings for the ‘celebrity’ angle it brings to them – especially terrorists out to make public statements. Surveillance should be targeted and on a balance between total cost and benefits, tilt to the latter. |  |
|  | 7 (f) | Delete this clause  OR  Replace it with “ where technically possible, use the Public Internet Protocol (IP) addresses for its computers | It is technically hard to enforce such a requirement since individuals might use anonymity tools to mask their IP addresses. |  |
|  | 7(g) | The retention guidelines should include security, confidentiality of log data collected and a ceiling date for retention. |  |  |
|  | 7 (i) | This might discourage organizations and businesses that offer public wireless services patrons from continuing with such due to the extra statutory requirements on this. Since cyber cafes are registered by the National Government as business entities and licenced by County governments for specific services. Instead of creating more authorization, some of these requirements can be incorporated in the existing licences at the time of renewal (for the existing) or application (for new applicants). |  |  |
|  | 11  (a) (b) (c) (d) (e)  (f) | Anonymity software, e.g. a Virtual Private Network (VPN) service with no-­‐log feature turned on + DNS Leak Protection easily outdo all the requirements under this section.  There should be a limited liability for service providers on this section since it is beyond them to technically enforce these requirements.  These requirements further criminalize privacy and anonymity online for individuals, a key component of security online and its attendant human rights. |  |  |
|  | 7 | This clause does not indicate the ceiling limits of retention |  |  |
| **Airtel** | 6(e) | The word download should be deleted | It may not be possible to know the contents of offensive material until the user downloads and views it |  |
|  | 7(b) | Not all devices that connect to wireless networks especially w-fi hotspots have mobile phone numbers, e.g. laptops, game consoles etc. all w-fi enabled devices can access a Wi-Fi hotspot even if they do not have a simcard. Secondly, you do not need a phone to access the services of a cyber cafe | The regulation is not practical and therefore we request that it is modified or removed all together. |  |
|  | 7(g) | The sentence is incomplete. A word is missing between the words “original” and “for”. Propose to insert the word “form” |  |  |
|  | 7(i) | The CA should review this regulation in view of device capabilities. | The regulation is not entirely practical as regards personal hotspots provided for using a mobile device. Users are able to share mobile hotspots from all their devices using the personal hotspots or tethering functionality. |  |
|  | 10 (1) | We need a definition of the word “public information” so that there is clarity in applicability and scope of this requirement |  |  |
|  | 11 | We propose that this is deleted or amended to incorporate the understanding of how OTTs work. | All the parts to do with Internet Telephony are not practical. Calls initiated from VOIP applications such as Skype, Whatsapp, Viber, Telegram Wire etc. do not have addresses attached to them as they ride on an existing internet connection and are only seen as data sessions so we cannot identify the initiators and recipients of calls made using these over the top applications (OTT) |  |
| **Sidney Ochieng** |  | Copyright-related offenses should be removed from the definition. The copyright law should be amended to add computer related violations. This may lead to outsized punishments for the mere mistake of uploading the wrong picture, video or audio online. | The potential damage caused by this compared to the others listed is minor. It is misplaced here |  |
|  | Part 4 | Part 4 Attack on Computer Systems makes no effort to distinguish between attempts and actual attacks. | Other laws have different sentences for attempts and actual attacks I don't see why this can't be the same for cyber crimes. Also the law makes no mention of intent which makes white-hats who discover vulnerabilities particularly exposed. This also applies to following section, 5 on Computerised Data Breaches. |  |
|  | 5 | Computerised Data Breaches part of, participate in an association formed or in an agreement established with a view to preparing or committing one or several of the offences provided for under this Convention. | Makes white hat groups vulnerable |  |
|  | 6 (f) | Threaten, through a computer system, to commit a criminal offence against a person for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of these characteristics;  The singular word gender is missing and should be added as discrimination against women is rampant. |  |  |
|  | 6(h) | “deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system. Should be removed. | It's vague, largely depends of the views of historians and also assumes to try to control how people think. |  |
|  | 7 | Operation and use of cybercafés and public wireless hotspots. | This entire section should be removed. It is wholly impractical and a violation of several constitutional rights particularly the one of privacy. The information collected can be arbitrarily demanded by the authority without a court order. It also adds yet another license to do business in part I  that will impede the ease of doing business. Further the meaning of public wireless hotspots is not defined at all. |  |
| **JTL** | 2 | Cyber café – the definition needs to be amended to note that a cyber café is any entity whose primary function is to offer internet access on a computer at a fee | The inclusion of the word “facility” makes the definition of cyber café vague. As a result, entities whose primary function is not to offer internet access at a fee are captured by this definition. |  |
|  | 2 | Public wi-fi hotspot | The definition is too narrow and should be expanded |  |
|  | (e) | Computerized data breaches – the clause should be deleted | The clause lacks clarity on what are the “Preliminary formalities to be complied with when processing computerised data” |  |
|  | (a) | Content related offence – amend to read:   1. Produce, register, offer, manufacture, make available, [knowingly] disseminate an image or a representation of child pornography through a computer system | The term “knowingly” should be included, so as to create the criminal intent. The term “transmit” should be deleted. Service providers are unable to control the images or representation transmitted through their computer system. In addition it will be very expensive to set up controls or measures that will monitor all images transmitted in their computer system. |  |
|  | 6 (b) | Should be amended to read  [knowingly] possess an image or representation of child pornography in a computer system or on a computer data storage medium. | The provision as it is does not provide for intent and fails to acknowledge that service providers may not have the knowledge or control of what its end users access/transmit through its computer system. |  |
|  | 7 | Operation and use of cyber cafes and public wireless hotspots – Prposal that there be separate clauses for operators of each. |  |  |
|  | 11 | Categories to be retained – proposal that this clause be deleted. | Service providers may not be able to implement the provision due to cost and capacity challenges. |  |
|  | 15 (c) | Jurisdictional provisions – the clause needs to be deleted to limit the jurisdiction of the Authority to only those offences committed by its nationals within Kenya. | The Authority is exceeding its mandate by giving itself jurisdiction over offences committed by Nationals outside of the country. |  |
|  | 20 (1) | Provision of access to third party material  The term “merely” should be deleted.  Amend the clause to read as follows:  A service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which heh or she provices access [hosts, transmits or stores] if the liability is founded on:   1. The making, publications, dissemination or distribution of the material or a statement made in the material; or 2. The infringement of any rights subsisting in or relation to the material | The use of the term “merely” diminishes the protection available to service providers who frequently provide additional services to its users.  The provision needs to also add the term “hosts, transmits and stores” in order to broaden the clause to include diverse types of intermediaries. |  |
|  | 21 | Information location tool  Amend the clause to read:   1. ..the service provider is not liable [pursuant to clause 20] if the service provider: 2. Removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed [receiving and considering a valid complaint under this part…] that the data message or the activity relating to the data message infringes the rights of the [complainant or the person on behalf of whom the complaint is made. | The activities of service providers for which the protection is intended includes a range of intermediary activities that goes beyond providing users with links to web pages. It includes storing, housing and transmitting information which has also been proposed in the amendment to clause 20. |  |
|  | 23 (1) | Service provider not obliged to monitor data  Delete – ‘for the purposes of complying with this part’  The clause to now read;   1. A service provider is not obliged to: 2. Monitor the data which service providers have transmitted or stored; or 3. Actively seek for facts or circumstances indicating an unlawful activity | This provision is not to be limited to the paragraph as it is a general proposition that is to apply to service providers at all times and in all circumstances. |  |
| **KEPSA** | 10 | It is proposed that paragraph 10 be deleted altogether. | The case for free flow of information.  All sectors of the economy benefit from the ability to move data across borders. Companies are able to send human resources data to and from headquarters, send data to R&D facilities set up abroad or use cloud-solutions to improve efficiency. For example, in the finance industry, consumers and small businesses globally can take advantage of market-leading financial services online  Mandating that the data be stored locally may be bad for security and bad for economic growth  Security:  Storing data online is safer than storing locally - Forced data localization doesn’t protect against foreign government surveillance. Storing data in one location could create a more attractive target.  Customers:  The services people use and depend on every day like YouTube, Google, Facebook, and Amazon might not be available locally if the burdens become too onerous or costly. Great new services are being developed all the time. Forced data localization may make it difficult for them to come to Kenya, if at all. The increased cost associated with data localization could lead to higher costs to customers (Brookings 2013), including schools and governments.  Business and the Economy:   * Forced data localization makes institutions less competitive and causes them to waste money because online storage reduces costs and complexity. According to a European Commission survey, 80% of organizations reduced costs by 10-20% as a result of online services and data storage (European Commission 2011). * The Internet adds over 3% to Kenya’s GDP and the government wants that number to triple by 2017. Just as setting up trade barriers will cause economic harm, so too will splintering of the Internet. * Forcing data centres to be built in a country does not create a significant number of jobs. Online services and other business sectors that rely on open data flows are a far more significant source of job growth. * Forced data localization impedes cross-border data flows which are essential for institutions, especially small- and medium-sized enterprises, to compete in the global economy. |  |
|  | Part III | Amend part III of the regulations by either:  a. Incorporating the amendments set out in the following part or;  b. Inserting an entirely new provision on intermediary liability protection in the manner set out in the amendments part below | * When intermediaries are exposed to the risk of criminal or civil liability for content on their networks, they are incentivized to control or police this content, and this has a chilling effect on both freedom of expression and the free flow of information, which is the lifeblood of the new information society and information economy. *[Source: APC Report: The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain, Alex Komninos, 2002]* * The risk that intermediaries face legal action for facilitating access to illegal content and by prescribing how much effort, in terms of compliance, intermediaries need to make to be considered exempt from liability, can influence the size and vibrancy of the Internet start-up and hence the e-commerce ecosystem *[The Economic Impact of Safe-Harbours in Internet Intermediary Start-ups - Oxera Study, 2015]* * Globally, investors see the legal environment as having the most negative impact on their investing activities, and early stage investors are particularly deterred from investing in the Digital Content Intermediaries in countries with insufficient ISP and safe-harbour protections *[The Impact of Internet Regulation on Early Stage Investment - Fifth Era study, 2014]* * It is therefore a positive step that the draft regulations propose to protect intermediaries from liability. Ideally, regulations on this subject would allow innovation and creativity online to thrive, such that online services can continue to empower a diverse range of content and speakers. |  |
|  | 26 | Provision of Access to Third-Party material  It is proposed to amend this clause in the manner set out in bold below:  *(1) A service provider shall not be subject to civil or criminal liability in respect of information to which he or she* ***~~merely~~*** *provides access,* ***[hosts, transmits, or stores]****, if the liability is founded on:-*   1. *the making, publication, dissemination or distribution of the material or a statement made in the material; or* 2. *the infringement of any rights subsisting in or in relation to the material;*   *(2): This Clause shall not affect –*   1. *An obligation in a contract* 2. *The obligation of a network service provider under a licensing or regulatory framework which is established by law; or* 3. *An obligation which is imposed by law or a court to remove, block or deny access to any material.* | Rationale for the amendments proposed to clause 26(1)   * Delete the term ‘merely’   The use of "merely" whittles down the protection available to service providers who frequently provide additional ancillary service. Such providers are not ‘merely’ providing the defined service. If an ISP provided some sort of content filtering, or reviewed content to block malicious content, then (counter-intuitively) it might lose its protection due to providing users with a higher quality service.   * Adding the terms ‘hosts, transmits, stores’   Broaden the clause to include the diverse types of intermediaries:   * The clause is limited to circumstances where the service provider is merely providing access to the information. This should be extended to cover circumstances where the service provider is hosting (i.e. storing on behalf of another) or acting as a conduit (i.e. transmitting the content on behalf of another); or hosting, transmitting and storage (not just temporary storage). |  |
|  | **Clause 27: Information location tools.** | The amendments proposed to this clause are set out in bold and strikethrough below:   1. *~~Where a~~* ***[A]*** *service provider ~~refers to or links users to a web page containing an intriguing~~* ***~~[infringing?]~~*** *~~data message or infringing activity, the service provider~~ is not liable* ***[pursuant to paragraph 26]*** *~~for damage incurred by the user~~ if the service provider-* 2. *~~does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user;~~* 3. *~~is not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;~~* 4. *~~does not receive a financial benefit directly attributable to the infringing activity~~; ~~or~~* 5. *removes or disables access to the reference or link to the data message or activity within a reasonable time after ~~being informed~~* ***[receiving and considering a valid complaint under this part….]*** *that the data message or the activity relating to the data message infringes the rights of the ~~user~~* ***[complainant or the person on behalf of whom the complaint is made].*** | Rationale for the amendments proposed to paragraph 27:   * Delete: *refers to or links users to a web page containing an intriguing data message or infringing activity* and replace with ‘pursuant to paragraph 26]   + The activities of service providers for which the protection is intended includes a range of intermediary activities that goes beyond providing users with links to web pages. It includes storing, hosting, and transmitting information, which has also been proposed in the amendments to paragraph 26. * Delete: *intriguing* and replace with ‘*infringing’*   + Presumably this is a typo.   + If it is not a typo, then it would violate constitutional guarantees of free speech for the Communications Authority to limit data or messages that it considers to be intriguing. * Delete: *‘does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user’*   + One of the foundations of intermediary liability protection is removing any presumption of a general obligation on intermediaries to monitor third party content. Already, paragraph 29 of the regulations recognizes this principle. This paragraph implies that an intermediary may have ‘actual knowledge’ of the infringing activity otherwise than through a proper notification by a complainant, which would be contrary to this principle and contradictory to paragraph 29. * Delete: is *not aware of the facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent*   + This is effectively a restatement of the obligation to monitor third party content, similar to the ‘actual knowledge’ clause, and for the same rationale, it should be deleted. * Delete: *does not receive a financial benefit directly attributable to the infringing activity*   + This clause takes away the protection that is intended by Part III. Service providers who render intermediary services (providing access to, hosting, transmitting or storing information on behalf of a third party) are a key business model in the ecommerce ecosystem. Their business models/fees structures are not based on the content of the third party data but on other factors such as the scale of resources provided e.g. internet speed, data size. Because no particular piece of data may be attributed with the service charge, the vagueness of this provision effectively takes away any form of protection.   + The provision places service providers under a general obligation to monitor third party content. Avoiding the risk of not complying with the provision would mean that a service provider will have to monitor the data on its networks in order to determine if there is any infringing data/activity. * Insert the words in bold: *removes or disables access to the reference or link to the data message or activity within a reasonable time* ***after receiving and considering a valid complaint under this part*** *that the data message or the activity relating to the data message infringes the rights of the* ***complainant or the person on behalf of whom the complaint is made***   + It would be cripple the operations of service providers (who include small and medium businesses providing innovative ICT services) if they are not protected from frivolous and vexatious complaints from persons who are not the subject of or have no legal or other interest in the data message. The complaints should be made in accordance with a mechanism set out in the regulations and by persons exercising a right in law, rather than by ‘users’ generally. |  |
|  | Paragraph 28 | Proposed amendments set out in bold and strikethrough:  *(1). A person who complains that* a data message or an activity relating to the data message *is unlawful shall notify the service provider or his or her designated agent in writing and the notification shall include –*   1. *the full name and address of the person complaining;* 2. *the written or electronic signature of the person complaining;* 3. *the right that has allegedly been infringed;* 4. *a description of the material or activity which is alleged to be the subject of infringing activity, including,* ***[in the case of material on a computer network or on the Internet, an electronic address, link or other information that uniquely identifies and locates the material]****;* 5. *~~the remedial action required to be taken by the service provider in respect of the complaint~~* 6. *telephone and electronic contact details of the person complaining;* 7. ***a court adjudication that the content is unlawful*** *or a declaration that the person complaining is acting in good faith,* ***has legal standing to assert the complaint and that the content is clearly and unambiguously unlawful****; and* 8. *a declaration that the information in the notification is correct to his or her knowledge.* 9. **a declaration that the complainant has made a reasonable effort, making use of the means and information publicly available, to contact the person or other entity responsible for making available the data message or activity and has asked to have it removed.**   *(2) A person who knowingly makes a false statement on the notification in subsection (1) is liable to the service provider for the loss or damage suffered by the service provider.* | Rationale for the amendments proposed to paragraph 28:   * Add *‘in the case of material on a computer network or on the Internet, an electronic address or other information that uniquely identifies and locates the material’*   + URLs - uniform resource locators - are electronic addresses that uniquely identify/locate information on the Internet. Including a URL link in the take-down request helps the intermediary to locate the information and to speedily resolve the complaint. Because there may be thousands or even millions of articles or data pieces on the Internet relating to a particular subject, it may not be possible for an Intermediary to honor a take-down request that purports to identify the information complained about merely by its subject matter. * Add the words in bold: *‘****a court has adjudicated that the content is unlawful*** or a declaration that the person complaining is acting in good faith, **has *legal standing to assert the complaint and that the content is clearly and unambiguously unlawful***   + Service providers, who are mostly private companies, should not be given the responsibility of adjudicating on whether the content is lawful or not. This should be left to judicial organs established by the state.   + It is important to protect service providers from frivolous and unjustified complaints made in bad faith or by persons having no legal interest in the subject matter of the complaint. * Delete sub-(e) *~~the remedial action required to be taken by the service provider in respect of the complaint~~*   + Since there are provisions in law on the remedial action that the intermediary should take with respect to the complaints, delete this sub-clause. * Insert: *a declaration that the complainant has made a reasonable effort, making use of the means and information publicly available, to contact the person or other entity responsible for making available the data message or activity and has asked to have it removed.*   + Since service providers serve an intermediary role on behalf of originators of data or information - providing data hosting, storage and transmission services - the complaint of first resort should be lodged with the person who originates, manipulates, updates and controls the data, ie, the originator.   + This may improve the response times in the removal of the information or the resolution of complaints and unburden the service provider with the responsibility of being an arbiter on whether the content is lawful or not, which is a responsibility that should be exercised by a judicial/government entity. |  |
|  | Proposed new paragraph | Insert the following new paragraph after paragraph 28.  ***29. Counter-notice***  *(1). If an information service provider receives a valid counter-notification, then it cannot be held liable for damages or other monetary relief for the content.*  *(b). A counter-notification is only valid if it meets the following criteria;*   1. *the entity or person submitting the counter-notification was accused of violating the law responsible for making available the data message or activity;* 2. *provides physical or electronic signature of the person or entity lodging the counter-notification, or a third-party authorized to act on their behalf; and* 3. *attests to the good faith and validity of the claim that the data message or activity is lawful or should otherwise not be taken down.* | Rationale for providing a counter-notice:   * As a matter of natural justice, the right to complain against online content should be balanced with the right of the originator of the content (or indeed any other person exercising a right in law) to oppose the complaint for valid legal reasons. * A counter-notice provision is a best-practice and is fundamental to a well-balanced, fair and workable intermediary liability protection regime. It has been applied and its benefits are self evident:   + It shields service providers from frivolous and baseless complaints;   It removes service providers - who are private entities - from the responsibility of adjudicating on the legality of online content, a responsibility that should be exercised through the state’s judicial authority. |  |
|  | 29 | **Service Provider not obliged to Monitor Data**  (1) ~~For the purposes of complying with this Part,~~  A service provider is not obliged to –   1. monitor the data which the service provider transmits, **[receives, provides access to, hosts]** or stores; or 2. actively seek for facts or circumstances indicating an unlawful activity.   ~~(2). The Authority may by statutory instrument, prescribe the procedure for service providers to-~~   1. ~~Inform the competent public authorities of any alleged illegal activities undertaken or information provided by recipients of their service; and~~ 2. ~~Communicate information enabling the identification of a recipient of the service provided by the service provider, at the request of a competent authority~~. | Rationale for the amendments proposed to paragraph 29:   * Delete: *‘for the purposes of complying with this part’*.   + The principles in this provision are not to be limited to the paragraph as they are general propositions that are to apply to service providers at all times in all circumstances. * Insert *‘receives, provides access, hosts’*   + This is to maintain consistency with clause 26(1) to capture the different types of service providers and the range of intermediary services provided by them. * Delete sub-clause (2)   + Necessarily, detecting 'alleged illegal activities' would mean that intermediaries such as ISPs would have to intercept and monitor private communications or data. This would not only place them in the position of law enforcement bodies but even more importantly, bring them into conflict with the constitutional protection of privacy.   + Since the clause provides that intermediaries are under no obligation to monitor their systems, then a *priori* they may not be placed under a general obligation to report ‘alleged illegal activities’ undertaken by the recipients of their service.   + This may have a chilling effect on e-commerce because trust is key for online business and social transactions. Users need an online environment in which they can trust in the privacy and confidentiality of personal information and communications. |  |
|  | Proposal to amend all of Part III | **Option B: Delete the existing provisions of Part III and substitute them with the following new provisions:**  In the alternative we propose supplanting the existing clause with a new one altogether as shown below:-   1. In this clause,   *“Information service provider*” means any natural or legal person who provides an information service;  *“Information service”* means any service at a distance by electronic means for the processing, storage, indexing, aggregation, transmission or provision of access to information, data or content originated by third parties;  “*Recipient of the service*” means any person who, for professional ends or otherwise, uses an information service, in particular for the purposes of seeking information or making it accessible.   1. Notwithstanding any provision contained in any law for the time being in force, an information service provider shall not be liable for any damages, monetary penalty, equitable relief or criminal sanction for any third party information, where:-    1. the information service provided by it consists in the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, where the service provider       1. did not initiate the transmission;       2. did not select the receiver of the transmission; and       3. did not modify the information contained in the transmission so as to alter the integrity of the information.    2. the information service provided by it consists in the storage of or provision of access to information provided by a recipient of the information service, where the service provider and upon obtaining notice in accordance with clause 5, acts expeditiously to remove or to disable access to the information, and    3. the information service provided by it consists in referring or linking recipients of the information service to the information by using information location tools, including a directory, index, reference, pointer, or hypertext link, where the service provider, upon obtaining notice in accordance with clause 5 acts expeditiously to remove or to disable access to the information. 2. For the purposes of sub-clause 2a), b) and c), any manipulations, compilation, aggregation of the information by the information service provider that does not alter the integrity of the information shall not prejudice the information service provider’s exemption from liability pursuant to clause 2). 3. An information service provider is under no obligation to monitor the information which it transmits, stores, provides access to, or otherwise processes in the course of providing an information service nor a general obligation actively to seek facts or circumstances indicating illegal activity. 4. In order for the notice referred to in sub-clause 2a) and b) to be valid, it must meet the following criteria,    1. a court of competent jurisdiction has adjudicated that the content is unlawful or that the complainant has legal standing to assert a claim (or is an agent acting on behalf of such a complainant) and that the content is clearly and unambiguously unlawful;    2. provides physical or electronic signature of a person authorized to act on his or her behalf    3. sets out the specific content to be removed, clearly identifying it by an electronic address or link where available, or other unique identifier;    4. attests to the good faith and validity of the claim using the legal form appropriate to the jurisdiction (such as an oath under penalty of perjury).    5. includes information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address;    6. attests that the complainant has made a reasonable effort, making use of the means and information publicly available, to contact the person or other entity responsible for making available the specific content to the Internet and has asked to have it removed. 5. If an information service provider receives a valid counter-notification, then it cannot be held liable for damages or other monetary relief for the content. 6. A counter-notification is only valid if it meets the following criteria;    1. the entity or person submitting the counter-notification was accused of violating the law, responsible for making available the specific content that was removed;    2. provides physical or electronic signature of the person or entity, or a third-party authorized to act on their behalf; and    3. attests to the good faith and validity of the claim that the information is lawful. 7. Any person who knowingly materially misrepresents under this clause,    1. that material or activity is unlawful, or    2. Causes the material or activity to be removed or disabled by mistake or misidentification, shall be liable for any damages, including punitive damages, costs and attorney's’ fees, incurred as a result. 8. An information service provider shall not be liable to any person for any claim based on the service provider’s good faith disabling of access to, or removal of, information, regardless of whether the information is ultimately determined to be legal or illegal. |  |  |
| **Control Risks** | Comments:  It’s not clear what the overarching purpose of these regulations are (they seem a strange mix of legislative provisions and regulations). It seems strange that offences and penalties are specified in regulations rather than primary legislation.  Most of the key definitions appear to be in line with the Budapest Convention on cybercrime (although we haven’t done a detailed mapping). | | |  |
|  | Definitions | Propose that the below definitions are adopted:  - Cyber-dependent crimes are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). These acts include the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks. They are activities primarily directed against computers or network resources, although there may be a variety of secondary outcomes from the attacks. For example, data gathered by hacking into an email account may subsequently be used to commit a fraud.  - “Cyber-enabled” crimes are those where the scale or nature of the offending has been transformed by technology, e.g. fraud.  - Neither category includes “traditional” crime (e.g. drugs trafficking) where criminals use ICT to communicate or for operational security (e.g. encryption), although specialist cybercrime resources are often called upon to assist in these cases |  |  |
|  | 5 (a) | There is no provision in Section 5(a) – prohibition of interception – for lawful interception by authorised bodies (e.g. police). |  |  |
|  | 7(c) | This is a massively sweeping power, and does not determine any due process behind this provision of user data. Who determines when it is necessary, for what purpose etc.? What safeguards are in place to protect abuse? |  |  |
|  | 9 | We understand that the Kenyan government wants to keep as much data as possible within Kenya and in local languages (making it easier to intercept/obtain where necessary), but the method for doing this is vague, nothing more than “The Authority shall facilitate the promotion of….” |  |  |
|  | 16(2) | A seven year prison sentence, or a fine, or both. Under what circumstances would a fine be levied rather than a prison sentence? Is there a risk that those able to pay will escape custodial sentences? As a parallel this issue was highlighted during an independent review of the Nigerian Cybercrime Bill. |  |  |
|  | Section 1 of Part 2 | Seems unnecessarily draconian; basically anyone in Kenya offering any online service has to receive an authorisation from the government. This does not help facilitate online business. |  |  |
|  | Part 1 – 4 (a) and (b) | Seem to be mutually inclusive and thus redundant if no penalties are defined at this stage. |  |  |
|  | 6(c) | Mentions the term data storage medium which is not defined in the regulation, it may need to be. |  |  |
|  | 7(c) | There is no provision indicating the duration for which cyber café and wifi hotspot owners should retain data for. Furthermore, does this regulation apply for mobile wifi hotspots too if it is left “open” (ie not password protected)? |  |  |
|  | 7(d) | Similarly there is no data retention duration for the client registry |  |  |
|  | 7(f) | Does this include both IPv4 and IPv6? Does this encompass both dynamic and static IP addresses? |  |  |
|  | 12 | As the data retention is for a minimum of 1 year in its original form, after that what format is acceptable? Only metadata or other formats? |  |  |
|  | Part II – Electronic commerce | This is massively restrictive and could discourage FDI or entrepreneurship in the country. |  |  |
| **Tespok** | Definitions | Cyber security definition is vague  Definition of E-commerce (page 4) was not clear and is already covered under the electronic regulations and should not apply to this particular regulation. Therefore they were wrongly repeated and we propose a review. | There is need to review the definitions so that its clear on who the target entities are and not to keep the definitions aligned to the KICA so that there is no confusion of interpretation  There is need to reduce the risk of misinterpretation as some of the regulations have clauses that are vague or ambiguous and rather ambitious. |  |
|  | Page 3 definitions | Critical Internet Resources was well defined but it could change with the change in technology |  |  |
|  | Page 5 definitions | There is need for more clarity on the definition of a service provider. i.e. who is a service provider?  This definition is also changing with different regulations and therefore creating confusion. It is important that if the regulations are in line with the current Act, they should also borrow definitions from the Act for purposes of uniformity |  |  |
|  | Page 5  PART 1 | The community is rather concerned about the regulations developing criminal offense that result in jail terms since criminal offense should be in the Act and the regulations should result in penalties and short jail terms in extreme cases. |  |  |
|  | See page 5  Part 1 on cyber Security  Offence 4 (d) | As the clause currently seats prohibits owners of computer systems from running their daily operations. We therefore propose the statement read “hinder , distort or attempt to hinder or distort the functioning of a computer system ………….without authorization from the owner |  |  |
|  | Page 6 : Computerized Data Breaches  Number 5(e) | We recommend to have a definition for preliminary formalities for clarity |  |  |
|  | Number 5(f) | Refers to a convention, “this Convention “but we are reviewing the regulations. |  |  |
|  | See page 9 part 6 (content related offences ) 6(a) | It was suggested that the word transmit should be removed and the word ‘unknowingly’ to be added at the end of the sentence.  Definition of computer system is too broad with no way of how monitoring can be facilitated. It is important for the drafting team to remember that owners of systems need to monitor, change and upgrade their computer system. |  |  |
|  | See page 9 Part 6 (content related offences) 6(c) | It is not in line with best practice  From a technical perspective it is not practical as it requires additional human resources that would not only be in breach of rights to privacy and cost the organization additional funds. |  |  |
|  | See page 9 Part 6 (content related offences) 6(e) | The regulation makes academic research illegal such as world War II materials illegal and this is counterproductive to the social development of the country. We propose that it include: “with the intent to commit a crime.”  Thus it will read: “….presentation of ideas or theories of racist or xenophobic nature through a computer system with the intent to commit a crime.” |  |  |
|  | See page 9 Part 6 (content related offences) 6(g) | The meaning of insult needs to be clarified. Since it is already covered in the penal code and persecutions have already happened to set precedence. This clause is not necessary. |  |  |
|  | See page 9 Part 6 (content related offences) 6(h) | This clause is not necessary if clause 6(e) is edited as proposed. |  |  |
|  | Page 6  Content related offences 6(a) | Operators do not have the authority to block pornography. Operators proposed to remove the word ‘transmit’ and add the word knowingly because the intent is important. |  |  |
|  | Content related offences 6(c) | Add the word knowingly to read “possess an image or representation of child pornography in a computer system or on a computer data storage medium knowingly.” |  |  |
|  | Content related offences 6(e) | This clause wills academic excellence because researchers will not be able to use archived information for research. Operators proposed the clause to read as “create, download, disseminate or make available in any form writings, messages, photographs, drawings or any other presentation of ideas or theories of racist xenophobic nature through a computer system with an illegal intent or purpose. | The needs to clarify how the technical operations of operators are run so as to enable CA develop appropriate, technically implementable regulations. |  |
|  | Content related offences 6(g) | The word ‘insult’ to be defined because it is ambiguous. |  |  |
|  | Content related offences 6(h) | Deliberately deny, approve or justify acts constituting genocide or crimes against humanity through a computer system –should be scraped off because it is already covered by AFRINIC |  |  |
|  | **PART II – INVESTIGATION OF** **CYBERCRIME OFFENCES** | We propose the regulations for cyber cafes and public wireless hotspots be separated for purposes of clarity and development or implementable regulations. |  |  |
|  | **Page 7**  (Operation and use of cyber Cafes and Public wireless hotspots) (a) | Clearly define cyber café and public wireless hotspots to protect home use, schools and universities that are affected by the proposed cyber café definition  There is need to have a distinction between free and paid internet access service.  Operators are willing to assist record customer information by a mechanism that allows for sending public Wi-Fi access codes to phones via sms or email with a one time password.  Not all devices have mobile number | The needs to clarify how the technical operations of operators are run so as to enable CA develop appropriate, technically implementable regulations. |  |
|  | See page 7 number (e) | Not practical to make implementation of public wifi impossible, there isn’t enough IP address space to achieve this |  |  |
|  | See page 7 number (g) | Define system logs and communication logs since the two different systems logs for an ordinary ISP may require upto 2.8 petabyte of disk space and this is when they are compressed. It is not possible to keep them as they are first viewed on the server. The cost of investment into the requirement is prohibitive to most service providers.  Logs must be compressed , clear definitions of what logs is  Cost of retaining such logs is high |  |  |
|  | See page 8: part 8: Management of critical internet recourses | We recommend deletion of this clause since it is a function of the Regional internet registry and part of the agreements of the RIR with LIRS |  |  |
|  | See page 8 Number 9 | We recommend a definition of local content |  |  |
|  | See page 8 1 Number 10: localization of Public information and Country Code Top level Domain Names | We recommend a definition of public information.  We recommend a definition of public body and government agencies. |  |  |
|  | See page 9 Number 11: Categories of data to be retained | (a) (ii) it is not technically possible to tie an address to a user  We recommend that CA review the cost implications of these regulations to operators. |  |  |
|  | See page 11:13 Data protection and Data security (d) | The data, except those that have been accessed and preserved , shall be destroyed at the end of the period of retention – other service providers may need the data for a longer period for later use and may not be able to destroy the data as indicated  We recommend the ‘shall’ in this clause to be replaced with ‘may’. |  |  |
|  | See page 11:14  Framework for reporting, investigating, prosecuting and managing cybercrime. | Part (c) (iii) We recommend that the clause should specify who should be given the access and to what extend? There should be a clear procedure of how access is to be handled and clarity on the use of court order or not. |  |  |
|  | See page 12:15 Jurisdictional Provisions | (i) C (ii) if the offense is committed outside the territorial jurisdiction of any country – The regulator has no legal authority to persecute crimes committed outside the country and we therefore recommend for revision of this clause accordingly. |  |  |