KICTANET

PROPOSALS FOR AMENDMENT OF THE COMPUTER AND CYBERCRIMES BILL 2017

Draft Document for Discussion – February 2018

Key words: Delete, amend, substitute, insert, add

Clause	Provision	Proposal	Justification
		Review of Existing provisions	
Recital	AN ACT of Parliament to provide for offences relating to computer systems; to enable timely and effective collection of forensic material for use as evidence, and facilitate international co-operation in dealing with cybercrime matters; and for connected purpose	AN ACT of Parliament to provide a framework for the enhancement of cyber security; prohibition, investigation and prosecution of cybercrime; coordination of cybersecurity; and for connected purposes.	Summarised for clarity.
2	Interpretation	Insert the following definitions as appropriate: “authorise” means to officially empower another with the legal right to perform an action. "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, software and communication facilities which are connected or related as a system or network;	These were previously included in the body of the Bill. They are better placed in the definition clause 2.

		"critical infrastructure" means vital virtual systems and assets whose incapacity or destruction would have a debilitating impact on the security, economy, public health and safety of the country; “child” means a person below the age of eighteen years; "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any - a) name, national identification number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number; b) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; c) unique electronic identification number, address, or routing code; or d) identification document issued by a government or private entity intended for the purpose of identification of individuals and duly completed with information concerning a particular individual; or e) electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument. “publish” means to distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange,	

		barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; “film” means a moving image in any form, whether or not the image has been altered in any way, that was originally captured by making a recording, on any medium, from which a moving image may be produced, and includes a copy of the image, “photograph” means a still image in any form, whether or not the image has been altered in any way, that was originally captured by photography, and includes a copy of the image.	
4		~~Insert new sub-section (4)~~ ~~(4) Any person who unlawfully and intentionally possesses data, or without reasonable cause, is found in possession of data, with the knowledge that such data was acquired unlawfully as contemplated in subsection (1), is guilty of an offence.~~	~~This addition deals with persons who may not have hacked but are in possession of the data that was hacked. Similar to handling offences in relation to stealing.~~ This could be a challenge for whistleblowers, as they would end up being prosecuted for the act.
6	Unauthorised interference 6. (1) A person who intentionally and without authorisation does any act which causes an unauthorised interference, to a computer system, program or data, commits an offence and is liable on conviction, to a fine not exceeding ten	Amend and replace clause 6(1) and (2) with new clauses 6 (1) and (2) as below: 6. (1) A person who intentionally and without authorisation, interferes with a computer system, program or data, commits an offence and is liable on conviction, to a fine not exceeding five million shillings	Revision intended to make the provision concise and define what interference constitutes. Recently cases people developing Bots, Malware, Ransomware are becoming common.

	million shillings or to imprisonment for a term not exceeding five years, or to both. (2) For the purposes of this section, an interference is unauthorised, if the person whose act causes the interference - is not entitled to cause that interference; does not have consent to interfere from a person who is so entitled. (3) A person who commits an offence under subsection (l) which,— results in a significant financial loss to any person; threatens national security; (C) causes physical injury or death to any person; or (d) threatens public health or public safety, is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both. (4) For the purposes of this section, it is immaterial whether or not the unauthorised interference is directed at any particular computer system, program or data; a program or data of any kind; or a program or data held in any particular computer system. (5) For the purposes of this section, it is immaterial whether an unauthorised modification or any intended effect of it is permanent or temporary.	or to imprisonment for a term not exceeding five years, or to both. (2) For the purposes of this section, “interference” means to permanently or temporarily – (a) delete, alter, damage, a computer system, program or data; (b) obstruct or deny access to a computer system, program or data; (c) interrupt or impair the functioning, confidentiality, integrity or availability of a computer system or program.	
8	**Illegal devices and access codes**	Amend section	The provision should also prohibit the rent or transfer of devices or programmes including such other

	8. (1) A person who knowingly manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data designed or adapted primarily for the purpose of committing any offence under this Part, commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.	Insert the words “rents, transfers,” immediately after “sells” Insert the words “a means of access or control” immediately before the word “designed” **Illegal devices and access codes** 8. (1) A person who knowingly **keeps**, manufactures, adapts, sells, **rents, transfers**, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data, or **a means of access or control** designed or adapted primarily for the purpose of committing any offence under this Part, commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding ten years, or to both.	means of access or control of computers to commit offences. This is especially relevant to tackling the use of botnets for criminal activity.
12	**False publications** A person who intentionally publishes false, misleading or fictitious data or misinforms with intent that the data shall be considered or acted upon as authentic, with or without any financial gain, commits an offence and shall, on conviction, be liable to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.	Delete clause 12	This provision constitutes an unjustifiable limit on the right. freedom of expression and opinion granted under the constitution. The UN Special Rapporteur & the UN Human Rights Committee have deemed such provisions unacceptable. In a world where people are writing, tweeting, whatsapping, texting, or blogging every minute, it would be grossly unreasonable to expect them to verify the truth of each

			statement published. This clause is reminiscent of section 29 of Kenya Information and Communication Act which was declared unconstitutional. It also fails the test set out in Article 24(2) of the Constitution with regard to legislation limiting a fundamental freedom.
13	13. (1) A person who, intentionally— (a) publishes child pornography through a computer system; (b) produces child pornography for the purpose of its publication through a computer system; or (c) possesses child pornography in a computer system or on a computer data storage medium, commits an offence and is liable, on conviction, to a fine not exceeding twenty million or to imprisonment for a term not exceeding twenty five years, or to both. (2) It is a defence to a charge of an offence under subsection (1) (a) protected computer system. or imprisonment term not exceeding twenty years or both. (3) For purposes of this section— “child” means a person under the age of eighteen years; “child pornography” includes data which, whether visual or audio, depicts—	Delete provision	The offence already exists and can be dealt with under Section 16 (Child pornography) of the Sexual Offences Act (2006) which is quite comprehensive.

	(a) a child engaged in sexually explicit conduct; (b) a person who appears to be a child engaged in sexually explicit conduct; or (c) realistic images representing a child engaged in sexually explicit conduct; "publish" includes to— (a) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; or (b) having in possession or custody, or under control, for the purpose of doing an act referred to in paragraph (a); or (c) print, photograph, copy or make in any other manner whether of the same or of a different kind or nature for the purpose of doing an act referred to in paragraph (a).		
15	Computer Fraud 13. (1) A person who, with fraudulent or dishonest intent — (a) unlawfully gains; (b) occasions unlawful loss to another person; or (c) obtains an economic benefit for oneself or for another person, through any of the means described in subsection (2), commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both.	Delete provision	Fraud is already provided for under numerous sections of the Penal Code – Sections 127 - Frauds and breaches of trust by persons employed in the public service; 313 - Obtaining by false pretences; 314 – Obtaining execution of a security by false pretences; 315 – Cheating; 316 – Obtaining credit, etc., by false pretences; 316B - Certain felonies by banks or other institutions; 317 - Conspiracy to defraud; 318.- Frauds on sale or mortgage of property;

	(2) For purposes of subsection (1) the word means refers to — (a) an unauthorised access to computer system , program or data; (b) any input, alteration, modification, deletion, suppression or generation of any program or data; (c) any interference, hindrance, impairment or obstruction with the functioning of a computer system; or (d) copying, transferring or moving any data or program to any computer system, data or computer data storage medium other than that in which it is held or to a different location in any other computer system, program, data or computer data storage medium in which it is held; or (e) uses any data or program; or has any data or program output from the computer system in which it is held, whether by having it displayed in any manner.		CHAPTER XXXII - Frauds By Trustees And Persons In A Position Of Trust, And False Accounting; 347 – making a false document; 348 – Intent to defraud; 352 - Forgery of, and other offences in relation to, stamps; 353 – Uttering false documents; 355 – procuring execution of documents by false pretences; 357 – making documents without authority In addition, a provision on aggravated offences is provided under clause 21, which already enhances the penalty for the use of computer systems in the commission of existing offences under the laws of Kenya.
14	Cyber-stalking and Cyber-bullying 14. (1) A person who, individually or with other persons, wilfully and repeatedly communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct— (a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; or (b) detrimentally affects that person.	Substitute the current clause 14 with the one as below: Cyber-Harassment 14. (1) A person who, individually or with other persons and whether directly or indirectly, wilfully and repeatedly communicates, contacts, monitors use of electronic communications, or spies on another person commits an offence, if they know or ought to know that their conduct—	These acts are becoming common within society. Individuals are known to stalk and harass others especially women, using SMS, Calls, Email and on social media networks causing them untold suffering. The provision also provide for granting of restraining orders by the courts to shield the victims from the continued harassment.

	(2) A person who commits an offence under subsection (1) is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both. (3) It is a defence to a charge of an offence under this section if the person establishes that— (a) the conduct was pursued for the purpose of preventing or detecting crime; (b) the conduct was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under the enactment; or (c) in particular circumstances, the conduct was in the public interest.	(a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property; (b) detrimentally affects that person; (c) amounts to harassment of that person; or (d) amounts to stalking of that person. (2) A person who commits an offence under subsection (1) is liable, on conviction, to a fine not exceeding three million shillings or to imprisonment for a term not exceeding three years, or to both. (3) It is a defence to a charge of an offence under this section if the person establishes that— (a) the conduct was pursued for the purpose of preventing or detecting crime; (b) the conduct was pursued under any enactment or rule of law or to comply with any condition or requirement imposed by any person under the enactment; or, (c) in particular circumstances, the conduct was in the public interest. (4) Where a person who is, or may be a victim of an offence under this section, or has an apprehension of the breach of the section, may apply to a court to make a restraining order against another person. The order will require the person complained of to refrain, for such period (including an indeterminate period), and from such conduct in relation to the victim or such persons as may be specified in the order.	

		(5) A person who, without reasonable excuse, contravenes an order made under this sub-section (4) is guilty of a misdemeanor.	
17	Aiding and abetting the commission of an offence 15. (1) A person who knowingly and wilfully aids or abets the commission of any offence under this Act commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both. (2) A person who knowingly and willfully attempts to commit an offence or does any act preparatory to or in furtherance of the commission of any offence under this Act, commits an offence and is liable, on conviction, to a fine not exceeding seven million shillings or to imprisonment for a term not exceeding four years, or to both.	Delete provision.	Under s.20 of the Penal Code, any person who aids, abets, counsels, or does the act constituting an offence or omits to do an act to facilitate an offence can be charged for the commission of the offence. Retaining would amount to repetition.
18(b)	**every person who at the time of the commission of the offence was a principal officer of the body corporate, or anyone acting in a similar capacity, is also deemed to have committed the offence, unless they prove the offence was committed without their consent or knowledge and that they exercised such diligence to prevent the commission of the offence as they ought to have exercised having regard to the nature of their functions and to prevailing circumstances, and is liable, on conviction,**	every person who at the time of the commission of the offence was a principal officer of the body corporate, or anyone acting in a similar capacity is also deemed to have committed the offence , and is liable on conviction, to a fine not exceeding three million shillings or imprisonment for a term not exceeding three years, or to both, unless they prove the offence was committed without their consent or knowledge and that they exercised such diligence to prevent the commission of the offence as they ought to have exercised having regard to the nature of their	seems clearer as paraphrased

	to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years, or to both.		
21	**Offences committed through the use of a computer System** 21. A person who commits an offence under any other law, through the use of a computer system, is liable on conviction, in addition to the penalty provided under that law to a fine not exceeding three million shillings or to imprisonment term for a term not exceeding four years, or to both.	Substitute current provision with a new clause 21 **Aggravated Factors in Computer-related Offences** 21(1). Where a person commits an offence under this Act, or any other law through the use of a computer system, or through any interference with data or a computer program, or computer system, then such person can be charged with an additional offence, and shall be liable on conviction, to an additional penalty, of similar description as the penalty provided under that law. (2). In determining whether to enhance an initial offence to an aggravated offence, the following factors shall be considered - impact and severity a) the nature and seriousness of the offence committed; b) whether the offence was committed for commercial advantage or private financial gain; c) the value involved, whether of the consequential loss or damage caused, or the profit gained from commission of the offence; d) the sophistication of the manner in which the offence was committed; e) whether there was breach of trust or responsibility;	The proposal modifies the description and matches the penalty under the provision to the penalty to that of the offence committed under the other law. This is so as to prevent a scenario where an original offence having a maximum sentence of 6 months, would be unduly enhanced to 4 years. It also provides a criteria for aggravating factors to be considered when charges/sentences are enhanced.

		g) whether the offence was committed by an individual or a group; h) the number of victims or persons affected by the offence; i) the conduct of the accused.	
Investigation Procedures			
24	24. (1) Subject to section 23, a police officer may, in special circumstances enter, without a warrant any premises in or on which the police officer suspects an offence under this Act has been or is likely to be committed, and take possession of such computer system. (2) Sections 119, 120 and 121 of the Criminal Procedure Code relating to execution of search warrant, and the provisions of that code as to searches apply to a search without warrant under this section. (3) For purposes of conducting a search under this section, the police officer shall carry with them, and produce to the occupier of the premises on request by that occupier, the police officer's certificate of appointment. (4) Where anything is seized under subsection (1), the police officer shall immediately make a record describing anything that has been seized, and without undue delay take or cause it to be taken before a court within whose jurisdiction the thing was found, to be dealt with according to the law.	Delete Provision	The provision does not fit the test provided under Article 24(2) of the Constitution. The right not to have your property searched is guaranteed under Article 31. Computer systems are not like physical buildings that you can enter and search. If not, properly done, there can be opportunity for abuse and compromising the evidence, in case of an ongoing investigation. The NIS Act already provides a procedure.

26	26 (6). Despite the provisions of this section, upon an application in writing by a police officer that demonstrates to the satisfaction of the designated Office of the Inspector- General of Police that there exist reasonable grounds to believe that specified subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control which is necessary or desirable for the purposes of any investigation, the designated Office may order such a service provider to submit subscriber information relating to such services in that service provider's possession or control.	Delete entire sub-section (6)	The provision violates the right to privacy. It lowers the threshold and renders the entire section meaningless as any situation can be made to fit into the exceptions. Thus it defeats the purpose of having a court process, provides an opportunity for abuse and cannot be remedied if the court order sought is not granted.
28	For purposes of subsection (1), real-time collection or recording of traffic data shall not be ordered for a period not exceeding six months.	Replace the word “six” appearing immediately after the word “exceeding” with the word “three.”	The goal is to reduce the duration of surveillance measures by the police to reasonable periods. The police should not have extensive periods to conduct surveillance if they do not have a case. The same power can be abused by police if it’s too extensive. Further, extension of time is allowed under sub-section (4).
	Interception of content data 29. (1) Where a police officer or an authorised person has reasonable grounds to believe that the content of any specifically identified electronic communications is required for the purposes of a specific investigation in respect of	Delete provision	This provision flies in the face of the right to privacy as enshrined under Article 31 of the Constitution, which provides inter alia that: Every person has the right to privacy, which includes the right not to have—

	a serious offence, the police officer or authorised person may apply to the court for an order to— permit the police officer or authorised person to collect or record through the application of technical means; compel a service provider, within its existing technical capability- to collect or record through the application of technical means; or to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications within the jurisdiction transmitted by means of a computer system. (2) In making an application under subsection (I), the police officer or an authorised person shall— state the reasons he believes the content data being sought is in possession of the person in control of the computer system; identify and state the type of content data suspected to be found on such computer system; identify and state the offence in respect of which the warrant is sought; state if they have authority to seek real-time collection or recording on more than one occasion is needed, and shall specify the additional number of disclosures needed to achieve the purpose for which the warrant is to be issued; explain measures to be taken to prepare and ensure that the real-time collection or recording is carried out-		(a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed.

	while maintaining the privacy of other users, customers and third parties; and without the disclosure of information and data of any party not part of the investigation; (U state how the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and (g) state the manner in which they shall achieve the objective of the warrant, real time collection or recording by the person in control of the computer system where necessary. (3) Where the court is satisfied with the grounds provided under subsection (2), the court shall issue the order applied for under subsection (1). (4) For purposes of subsection (I), the real-time collection or recording of content data shall not be ordered for a period that exceeds the period that is necessary for the collection thereof and in any event not for more than a period of nine months. (5) The period of real-time collection or recording of content data may be extended for such period as the court may consider necessary where the court is satisfied that— such extension of real-time collection or recording of content data is required for the purposes of an investigation or prosecution; the extent of real-time collection or recording of content data is proportionate and necessary for the purposes of investigation or prosecution: despite prior authorisation for real-time collection or recording of content data, further real-time collection or recording of content data		

	is necessary to achieve the purpose for which the warrant is to be issued; measures shall be taken to prepare and ensure that the real-time collection or recording of content data is carried out while maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; the investigation may be frustrated or seriously prejudiced unless the real-time collection or recording of content data is permitted; and the cost of such real-time recording and collection is not overly burdensome upon the person in control of the computer system. The court may also require the service provider to keep confidential the order and execution of any power provided for under this section. A service provider who fails to comply with an order under this section commits an offence and is liable, on conviction— where the service provider is a corporation, to a fine not exceeding ten million; in case of an officer of the service provider, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.		

		Part Iv-International cooperation	Comments(from current group discusssion)
33,34			Can we instead have a wider definition of data that captures all types of data. today we have traffic/stored data, tomorrow we may have totally different types of data. Also if we look at blockchain, there's both the component of traffic and stored data
	General to the entire part Part (iv)		The glue that holds this together is a proper data protection law,for example,the bill provides for sharing of information with other states but **subject to** our laws , which other laws?the data protection Act would have made sense here
	General to the entire part Part (iv)		there needs to be adequate assessment of regional instruments to compare and contrast with the bill. We were not able to do that in this sitting
	38. A police officer or another authorised person may, without the authorisation but subject to any applicable provisions of this Act—	Delete the phrase "(Open source)"	

	access publicly available (open source) stored computer data, regardless of where the data is located geographically; or		

Proposals for Additional Clauses

Clause	**Provision**	**Proposal**	**Justification**
New Clause		Insert new clause The Cabinet Secretary responsible for internal security, in consultation with the relevant agencies responsible for the administration of justice, shall within six months of the commencement of this Act, develop Standard Operating Procedures and Guidelines for the conduct, search, seizure and collection of electronic evidence.	It is important to have a clear standard procedure for the collection of electronic evidence by law enforcement agencies.
New Clause		Insert new clause Limitation to the right to privacy (1) The right to privacy set out in Article 31 of the Constitution, may be limited in respect of a person who is subject to investigation or suspected to have committed an offence to the extent that subject to	Any limitation of rights under the Constitution, is subject to Article 24 and as such must be expressly provided for by Statute

		provisions of this Act relating to Warrants, the privacy of a person's home, property, possessions, information and communications may be investigated, monitored or otherwise interfered with. (2) The police shall, prior to taking any action contemplated under this section, obtain a warrant under this Act.	
New clause		Insert new clause **Online Grooming** (1) A person who, being an adult or while pretending to be a child – (a) communicates to a child by means of information communication technology; (b) proposes, prepares, encourages or solicits to meet the child; (c) knowing such child to be below the age of 18 years; and, (d) for the purpose of obtaining sexual gratification or engaging in sexual activities with the child, or for the purpose of committing the offences under section 11; commits an offence and shall be liable upon conviction to a term of imprisonment not exceeding five years or to a fine not exceeding five million shillings or both. (2) For purposes of this section, "sexual activity" means an activity that a reasonable person would, in	This is becoming an issue for concern in the country and needs to be addressed. This is especially so in Urban and coastal areas e.g. Kwale where foreign tourists get in touch with minors via phone, SMS, Whatsapp, SnapChat or Facebook and induce to engage in sexual activities. These are then recorded and distributed as child pornography.

		all the circumstances but regardless of any person's purpose, consider to be sexual.	
New Clause		~~Insert new clause~~ ~~**Child Sex Tourism**~~ ~~A person who advertises, promotes, makes arrangements or travels from their usual environment to a destination locally or abroad for the purpose of sexually exploiting, having sexual contact with children, or child pornography commits an offence and shall be liable upon conviction to a term of imprisonment not exceeding ten years or to a fine not exceeding five million shillings or both.~~	~~This is becoming an issue for concern in the country and needs to be addressed.~~
New Clause		Insert new clause **Identity theft** A person who fraudulently, dishonestly or without lawful authority, transfers or makes use of the electronic signature, password, means of identification or any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to a term of imprisonment not exceeding ten years or both.	This is becoming an issue for concern in the country and needs to be addressed.
~~**New Clause**~~		~~Insert new clause~~ ~~**Cyber Squatting**~~	~~This is becoming an issue for concern in the country and needs to be addressed.~~

		~~(1) A person who intentionally registers, traffics in, or uses a domain name –~~ ~~a) without any right or legitimate interest in the domain name;~~ ~~b) which is identical or similar to be confused with a trademark;~~ ~~c) which is dilutive of a trademark; or,~~ ~~c) in bad faith.~~ ~~commits an offence and is liable to a fine not exceeding three hundred thousand shillings.~~ ~~(2) Where a person is convicted under sub section (1), a court shall order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.~~ ~~(3) A charge under this provision does not limit the rights of a complainant to a civil action under the Trademark Act.~~	
New Clause		Insert new clause **Disclosure of private photograph or film** (1) A person who - (a) records or discloses a private photograph or film without the consent of an individual who appears in the photograph or film, with the intention of causing	This is becoming an issue for concern in the country and needs to be addressed.[1] Individuals are known to secretly take photos and film either their sexual partners or other people and make those recordings public to annoy their former partners once their

[1] Ex boyfriend to dethroned Miss Kenya 2016 to pay Sh1 million for leaking her nude photos, Dec. 13, 2016, ELLY GITAU, The Star. See: http://www.the-star.co.ke/news/2016/12/13/ex-boyfriend-to-dethroned-miss-kenya-2016-to-pay-sh1-million-for_c1472981

		that individual distress, commits an offence and is liable to imprisonment for a term of three years or to a fine not exceeding three million shillings, or both. (b) threatens to disclose or distribute a private photograph or film, or intends to arouse a fear that the threat will be, or is likely to be carried out, or is recklessly indifferent as to whether such a fear is aroused, commits an offence and is liable to imprisonment for a term of not exceeding one year or to a fine not exceeding one million shillings, or both. (3) Where a person is convicted under this section, a court may make such orders to prohibit the distribution or mandate the removal, retraction, deletion and destruction of such photograph or film from any platform by the person in contravention within a specified period. A person who, without reasonable excuse, contravenes an order made under sub-section (3) is guilty of a misdemeanor. (4) For purposes of this section – (a) “private photograph or film” means – an actual, or an altered photograph or film appearing to show a person in a state of undress, a person’s private parts, a person engaged in a sexual act not ordinarily done in public, or in circumstances in which	relationship ends. It can also be used as a means to extort individuals for payment. The provision also provide for granting of orders by the courts to prohibit distribution and mandate deletion of the content.

		a reasonable person would reasonably expect to be afforded privacy. (b) It shall not be an offence under this section if the conduct alleged to constitute the offence was done – i) for a genuine medical or scientific purpose, ii) for a genuine law enforcement purpose, by a law enforcement officer, or iii) in circumstances that a reasonable person would consider the conduct of the accused person acceptable.	
New clause		Insert new clause **[Social Engineering] attack -** **Improper use of computer system** **abuse of social engineering** **Pre-texting** A person who tricks or psychologically manipulates another into performing actions on a computer system or divulging confidential information, or for the purpose of the commission of a crime, commits an offence and is liable upon conviction to a fine not exceeding five million shillings or to a term of imprisonment for a term not exceeding five years or both.	This is a type of confidence trick for the purpose of information gathering, fraud, or system access. It is often more of a complex fraud scheme. It includes making up of fake profiles or pages on social network sites and websites. It can be used to obtain login credentials and impersonate individuals in financial services e.g. online banking and online transactions causing harm or financial loss to a person.
New clause		Insert New Clause	

		Reporting on Prosecutions The Director of Public Prosecutions shall report to the Parliament annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under this Act	
New Clause		**Duties of persons collecting Personal data** Any person collecting and storing personal data through a computer system, shall ensure that the data – a) is obtained, processed and stored only for specified lawful purposes; b) collected with the prior informed consent and is relevant and compatible with the purpose intended and is not excessive; (c) is not processed or kept longer than is necessary for the purpose that it was intended; (d) is securely stored using appropriate technical and organisational measures to prevent unauthorised access, accidental loss or destruction, or damage. (e) is not arbitrarily transferred to jurisdictions without adequate level of protection; and, (f) is accurate and where necessary, kept up to date.	Increasingly, many institutions are collecting, processing and storing personal data in electronic format. These include in financial, health, education, and for commercial services. This also includes CCTV and other surveillance footage. This information is usually the subject of cyber-attacks and as such, should be properly safeguarded. Therefore this places a responsibility on persons collecting such data to observe certain standards to ensure its security.
New Clause		Insert new clause **Unlawful obtaining and disclosure of personal data**	This is proposed so as to deal with persons or organizations who are reckless or knowingly trading or sharing personal data collected by

		(1) A person who knowingly or recklessly and without the consent of the subject of the personal data or their representative - (a) obtains or discloses personal data or the information contained in personal data; (b) procures the disclosure to another person of the information contained in personal data; or (c) sells personal data. commits an offence and is liable upon conviction to a fine not exceeding three million shillings or to a term of imprisonment for a term not exceeding three years or both. (2) It shall not be an offence under this section if the obtaining, disclosing or procuring— (a) was necessary for the purpose of preventing or detecting crime; (b) was required or authorised by or under any enactment, by any rule of law or by the order of a court; (c) was done under a reasonable belief of a consent or a right to obtain, disclose or procure the data; or, (d) was done in the public interest having regard to the obtaining circumstances.	them in trust for purposes other than which was intended.

New clause		**Minister to develop framework** The Minister shall within two-years of the coming into force of this Act, develop an appropriate policy and legal framework to safeguard the security of personal data.	
New Clause		Insert new clause **Liability of Legal Persons** (1) A legal person may be held liable for any of the offences under this act committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on: (a) a power of representation of the legal person; (b) an authority to take decisions on behalf of the legal person; or (c) an authority to exercise control within the legal person. (2) A legal person may be held liable where the lack of supervision or control by a person referred to in subsection 1 has made possible the commission, by a person under its authority, of any of the offences under this Act for the benefit of that legal person. (3) The liability of legal persons under this section shall be not prejudice the initiation of criminal proceedings against natural persons who are perpetrators, inciters or accessories to the offences.	Intermediary liability is an important question for discourse among actors. It is necessary to limit the liability of intermediaries e.g. telcom companies, ISP and other online service providers against the actions of users of their services.

		(4) A court which finds a legal person culpable under this section, may order: a) Temporary or permanent disqualification of the legal person from practicing commercial activities; b) The legal person to take such appropriate measures under the courts supervision; c) Winding up of the legal person; or, d) Temporary or permanent closure of establishments used to commit the offence.	
New Clause		Insert new clause **Establishment of a National Cybersecurity Council** (1) There is established an unincorporated body to be known as the National Cybersecurity Council. (2) The Council shall be composed of— (a) the Cabinet Secretary for the time being responsible for matters relating to the Information and Communication Technology, or his or her representative appointed in writing, who shall be the Chairperson; (b) the Attorney-General, or his or her representative appointed in writing; (c) the Director of Public Prosecutions, or his or her representative appointed in writing; (d) the Director-General of the Communications Authority, or his or her representative appointed in writing;	It is important to establish a multi-stakeholder body to review and coordinate the actions by state and non-state actors on cybersecurity.

		(e) the Inspector-General of the National Police Service, or his or her representative appointed in writing; (f) the Principal Secretary for the time being responsible for matters relating to Internal Security or his or her representative appointed in writing; (g) the Principal Secretary for the time being responsible for matters relating to Trade or his or her representative appointed in writing; (h) the Principal Secretary for the time being responsible for matters relating to Science and Technology or his or her representative appointed in writing; (i) the Principal Secretary for the time being responsible for matters relating to Defence or his or her representative appointed in writing; (j) the Governor of the Central Bank of Kenya or his or her representative appointed in writing; (k) a representative of an organisation or association dealing with information security; (l) a representative of an organisation or association dealing with human rights issues; (m) a representative of an organisation or association dealing with internet policy issues; (n) a representative of an organisation or association dealing with telecommunication services; (o) a representative of an academic institution dealing with information security; (p) a representative of an organisation or association dealing with the media; (q) a representative of the Law Society of Kenya;	

		(r) a representative of telecommunication service providers; and (s) a representative of a professional organisation or association dealing with the Information Communication Technology. (3) The Director-General of the Communication Authority shall be the secretary to the Council. (4) The Communications Authority shall provide secretariat services to the Council. (5) Not more than two-thirds of the members of the Council shall be of one gender and the Chairperson of the Council shall, during the first meeting of the Council, ensure that this requirement has been met. (6) The persons nominated under this section shall be appointed by the Cabinet Secretary from organisations with national coverage and known track records in their respective fields and shall serve for a term of three years which may be renewed for one further term of three years.	
New Clause		Insert New clause **Purpose of the National Cybersecurity Council** (1) The Council shall ensure a co-ordinated, efficient, effective and consultative approach in the coordination of cybersecurity initiatives.	This provides the purpose and functions of the Council

		(2) To achieve the objectives set out under subsection (1), the Council shall: a) formulate policies relating to the coordination of cybersecurity; b) implement, monitor, evaluate and review strategies for the cybersecurity; c) encourage collaboration among academics, researchers, engineers, industry and government in cyber security; d) encourage innovation in the field of cyber security, protecting assets, content and infrastructure from malicious attack or unintentional exposure; e) reduce risks to the country by working with public and private sector organizations to improve their cybersecurity; f) understand the cybersecurity environment, share knowledge, and use that expertise to identify and address systemic vulnerabilities; g) offer cyber security advice and guidance to government and other organizations; h) provide unified, coherent, collaborative and effective response to cyber security; and, i) conduct research and surveys to inform the country's approach to cyber security.	
New Clause		The functions of the National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC) shall be to:	

		a) respond to cyber security incidents to reduce the harm they cause b) advise on Cybersecurity matters c) coordinate cyber incident response in collaboration with relevant actors locally, regionally and internationally; d) act as the national trusted point of contact for information security matters; e) gather and disseminate technical information on computer security incidents; f) Carry out research and analysis on computer security; g) Create awareness on cybersecurity-related activities; h) provide independent assessment of threats and vulnerabilities i) Facilitate the development of a National Public Key Infrastructure (NPKI). j) To support the wider national campaign to grow the Kenya's cyber security capability and capacity k) To develop information sharing programme with public and private institutions l) To be the lead agency in the country with overall responsibility for cyber security advice.	
New Clause		The functions of the cybercrime unit shall be to: a) To serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. b) To provide victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations.	

		c) To provide a central referral mechanism for complaints involving Internet related crimes. d) Protection of digital citizens	

General Comments from Group 3:

1. Penalties. We have noted that the penalties are varied even for similar offences. Further, penalties for some offences (eg identity theft) are not commensurate to the offence. This needs harmonization.
2. Some of the offences (espionage, fraud) are covered in other pieces of legislation eg Penal Code. We propose:
    (a) Deleting these clauses and amending those other laws to reflect the aspect of using computer systems to commit the crime
    (b) Create an offence similar to 'aiding and abetting' that covers offences committed through the use of computer system.
    (c) Leave them in the Bill