Approved for tabling
SNA
20/3/18

REPUBLIC OF KENYA

THE NATIONAL ASSEMBLY

TWELFTH PARLIAMENT - SECOND SESSION

THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION

REPORT ON CONSIDERATION OF THE COMPUTER AND CYBERCRIMES BILL, 2017

DIRECTORATE OF COMMITTEE SERVICES
CLERK'S CHAMBERS
PARLIAMENT BUILDINGS
NAIROBI-KENYA

March, 2018

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

CAK	Communications Authority of Kenya.
Cap.	Chapter.
CIPIT	Centre for Intellectual Property and Information Technology Law.
ICT	Information and Communication Technology.
ICTAK	Information Communication Technology Association of Kenya.
ISACA-Kenya	Information System Audit and Control Association – Kenya Chapter
KEPSA	Kenya Private Sector Alliance.
KICA	Kenya Information and Communications Act.
KICTANET	Kenya ICT Action Network.
TESPOK	Technology Service Providers of Kenya.

ANNEXTURES

Annexture 1 National Assembly Advertisement in the Daily Nation and Standard Newspapers dated 6th February, 2018

Annexture 2 Minutes

Annexture 3 Adoption List

Annexture 4 Memorandum submitted to the Committee by ISACA-Kenya.

Annexture 5 Memorandum submitted to the Committee by KICTANET.

Annexture 6 Memorandum submitted to the Committee by Media Council of Kenya.

Annexture 7 Memorandum submitted to the Committee by CIPIT.

Annexture 8 Memorandum submitted to the Committee by the Communication Authority of Kenya.

Annexture 9 Memorandum submitted to the Committee by KEPSA.

Annexture 10 Memorandum submitted to the Committee by ICTAK.

Annexture 11 Memorandum submitted to the Committee by SOTE Hub.

Annexture 12 Memorandum submitted to the Committee by TESPOK.

Annexture 13 Memorandum submitted to the Committee by Mr.Michael Otieno.

Annexture 14 Memorandum submitted to the Committee by Safaricom Limited.

Annexture 15 Memorandum submitted to the Committee by Article 19.

Annexture 16 Memorandum submitted to the Committee by the Ministry of Information, Communication and Technology

THE CHAIRPERSON'S FOREWORD

The Departmental Committee on Communication, Information and Innovation is established and mandated under Standing Order No.216 to *inter alia*; 'Study and review all the legislation referred to it'.

The Computer and Cybercrimes Bill, 2017 a Bill for an Act of Parliament sponsored by Hon. Aden Duale, was read a first time on 10th October, 2017 and subsequently referred to the Departmental Committee on Communications, Information and Innovation for consideration and thereafter report to the House pursuant to Standing Order No.127(1).

The Committee placed an advert in the local dailies and wrote to the key stakeholders inviting them to submit their views on the Bill.

Upon receipt of the memoranda, the Committee held several meetings where they met with the stakeholders to consider the submissions received as incorporated in this report. A total thirteen (13) memoranda were received from members of the public and institutional stakeholders in the ICT sector through the Offices of the Clerk of the National Assembly. The Committee further held two meetings with the Ministry of Information, Communications and Technology and the Kenya ICT Action Network, respectively, to interrogate the history and justification for the Bill as well as its relevance to the current Information and Communication Technology space.

Thereafter, the Committee proceeded for a report writing retreat which provided the opportunity to consider the submissions of the public and stakeholders and to further draft, consider and approve its Report.

Acknowledgements

The Committee appreciates the assistance provided by the Office of the Speaker and of the Clerk of the National Assembly that enabled it to discharge its functions in considering the Computer and Cybercrimes Bill, 2017.

I take this opportunity to thank all Members of the Committee for their input and valuable contributions during the deliberations of the submissions by different stakeholders on the Computer and Cybercrimes Bill, 2017.

Pursuant to provisions of Standing Order 199 (6), and on behalf of the Departmental Committee Communication, Information and Innovation, it is my pleasant privilege and honor to present to this House the Report of the Committee on its consideration of the Computer and Cybercrimes Bill, 2017.

SIGNED.....

HON.WILLIAM KISANG, MP
(CHAIRPERSON)

COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION

DATE: 20/03/2018

PREFACE

Committee Mandate

The Departmental Committee on Communications, Information and Innovation is established under *Standing Order 216* whose mandate pursuant to the Standing Order 216 (5) is as follows;

a. Investigate, inquire into, and report on all matters relating to the mandate, management, activities, administration, operations and estimates of the assigned Ministries and departments;

b. Study the programme and policy objectives of Ministries and departments and the effectiveness of the implementation;

c. Study and review all legislation referred to it;

d. Study, assess and analyze the relative success of the Ministries and departments as measured by the results obtained as compared with their stated objectives;

e. Investigate and inquire into all matters relating to the assigned Ministries and departments as they may deem necessary, and as may be referred to them by the House;

f. To vet and report on all appointments where the Constitution or any law requires the National Assembly to approve, except those under Standing Order 204 (*Committee on Appointments*);

f (a) examine treaties, agreements and conventions;

g. make reports and recommendations to the House as often as possible, including recommendation of proposed legislation;

h. make reports and recommendations to the House as often as possible, including recommendation of proposed legislation;

i. consider reports of Commissions and Independent Offices submitted to the House pursuant to the provisions of Article 254 of the Constitution; and

j. Examine any questions raised by Members on a matter within its mandate.

In accordance with Second Schedule of the Standing Orders, the Committee is mandated to oversee Communication, Information, media and broadcasting (except for broadcast of parliamentary proceedings), Information Communications Technology (ICT) development and advancement of technology and modernization of production strategies.

Committee Membership

1. The Hon.Kisang William Kipkemoi, M.P - **Chairperson**
2. The Hon.George Macharia Kariuki, M.P - **Vice Chairperson**
3. The Hon.Liza, Chelule Chepkorir, M.P.
4. The Hon.Alfah, O. Miruka, M.P.
5. The Hon.Annie Wanjiku Kibeh, M.P.
6. The Hon.Joshua Kimilu, Kivinda, M.P.
7. The Hon.Marwa Kitayama Maisori, M.P.
8. The Hon.Mwambu Mabongah, M.P.
9. The Hon.Maritim Sylvanus, M.P.
10. The Hon.Mwangaza Kawira, M.P.
11. The Hon.Jonah Mburu, M.P.
12. The Hon.Gertrude Mbeyu Mwanyanje , M.P.
13. The Hon.Wamuchomba, Gathoni, M.P.
14. The Hon.(Eng)Mark Nyamita Ogola,M.P
15. The Hon.John Kiarie Waweru, M.P.
16. The Hon.Erastus Nzioka Kivasu, M.P.
17. The Hon.Innocent Momanyi, Obiri, M.P.
18. The Hon.Godfrey Osotsi, Atieno , M.P.

19. The Hon.Anthony, Tom Oluoch, M.P.

Committee Secretariat

1.	Mr. Nicholas Emejen	Deputy Director Committee Services (Lead Clerk)
2.	Ms. Ella Kendi	Third Clerk Assistant
3.	Mr. Ronald Walala	Legal Counsel II
4.	Ms. Lorna Okatch	Research Officer III
5.	Ms. Catherine Gati	Fiscal Analyst III
6.	Mr. Wilson Angatangoria	Sergeant at arms

CHAPTER ONE

INTRODUCTION

1.1 Background

1. The Computer and Cybercrimes Bill, 2017 sponsored by the Leader of the Majority Party, the Hon. Aden Duale, MP, was read a first time on 10th October, 2017 and subsequently referred to the Departmental Committee on Communications, Information and Innovation for consideration and thereafter report to the House.

1.2 Overview of the Bill

2. The Computer and Cybercrimes Bill, 2017 seeks to provide for offences relating to computer systems in order to enable timely and effective detection, investigation and prosecution of computer and cybercrimes, including in collaboration with other states under mutual legal assistance agreements. The pertinent content of the Bill are as follows—
3. Clause 2 of the Bill contains the definition of terms used in the Act. The responsible Cabinet Secretary for the Act is defined as the Cabinet Secretary responsible for matters relating to Information, Communications and Technology.
4. Clause 3 of the Bill outlines the objects of the Bill as the protection of the confidentiality, integrity and availability of computer systems, programs and data; prevention of the unlawful use of computer systems; facilitation of investigation and prosecution of cybercrimes; and facilitation of international cooperation on the subject matter of the Bill.
5. Part II of the Bill outlines the various offences proscribed under the Bill. These are—
    (a) Unauthorized access of a computer system which is punishable with the imposition of a fine not exceeding five million shillings or a term of imprisonment not exceeding three years, or both;

(b) Access of a computer system with intent to commit or facilitate the commission of a criminal offence which is punishable with the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding ten years, or both;

(c) Unauthorized interference with a computer system, program or data which is punishable with the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both. Where the interference results in a significant financial loss to a person, threatens national security, causes physical injury or death to a person or threatens public health or public safety, the penalty is enhanced to a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(d) Unauthorized interception of data to or from a computer system over a telecommunication system which is punishable with the imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(e) Manufacture, adaptation, sale procurement for use, importation, offering to supply, distribution or otherwise making available for use a device, program, computer password, access code or similar data for the purpose of committing an offence under the Bill which is punishable with the imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding five years, or both. A person who without sufficient justification receives a device, program, computer password, access code or similar data for the purpose of committing an offence under the Bill also commits an offence punishable with the

imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both;

(f) Unauthorized disclosure of a password, access code or other means of gaining access to a program or data held in a computer system which is punishable with the imposition of a fine not exceeding five million shillings or a term of imprisonment not exceeding three years, or both. Where the disclosure is intended for a wrongful gain, an unlawful purpose or to occasion any loss, the penalty is enhanced to the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both;

(g) Unauthorized access, interference with or interception of data to or from a protected computer system which is punishable with the imposition of a fine not exceeding twenty five million shillings or a term of imprisonment not exceeding twenty years, or both;

(h) Cyber espionage which is punishable with the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding twenty years, or both;

(i) Publishing false, misleading or fictitious data with the intention that the data be considered or acted upon as authentic which is punishable with imposition of a fine not exceeding five million shillings or a term of imprisonment not exceeding two years, or both;

(j) Publication, production or possession of child pornography on a computer system which is punishable with imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding twenty five years, or both;

(k) Forgery of computer data resulting in inauthentic data with the intention that the data be acted upon for legal purposes as if authentic which is punishable with imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both. Where the forgery is intended for wrongful gain, wrongful loss to another person or economic benefit, the penalty is enhanced to a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(l) Cyberstalking and cyberbullying which are punishable with imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(m) Aiding or abetting the commission of an offence under the Bill which is punishable with imposition of a fine not exceeding seven million shillings or a term of imprisonment not exceeding four years, or both;

(n) Commission of an offence under the Bill by a body corporate punishable with imposition of a fine not exceeding fifty million shillings to the body and a fine not exceeding five million shillings or a term of imprisonment not exceeding three years, or both on the principal officer of the body; and

(o) Commission of an offence provided for under any other law through a computer system which is punishable with, in addition to the penalty provided under that law, imposition of a fine not exceeding three million shillings or a term of imprisonment not exceeding four years, or both.

6. Clause 23 of the Bill allows a police officer or an authorized person to apply to court for a warrant of search and seizure of stored computer data during the course of investigating offences under the Bill.
7. Clause 24 of the Bill empowers a police officer or authorized person, in special circumstances, to without warrant enter intoa premises in which he or she suspects an offence under the Bill has been or is likely to be committed and take possession of a computer system. The police officer or authorized person must identify him or herself to the owner of the premises, record in writing anything seized and without delay cause anything seized to be taken before court.
8. Clause 26 of the Bill empowers a police officer or an authorised person to apply to court for a production order for specified data stored in a computer system or a computer data storage medium in the possession or control of a person or specified subscriber information relating to services offered by a service provider in Kenya in that service provider's possession or control where the data or information is necessary or desirable for the purposes of an investigation.
9. Clause 27 of the Bill empowers a police officer or authorised person to serve a notice for the preservation or disclosure of information in a person's possession that may be at risk of being modified, lost, destroyed or rendered inaccessible. The person served with the notice is obliged to ensure the preservation of the information.
10. Clause 28 of the Bill empowers a police officer or authorised person to apply to court for an order to permit the collection or recording of traffic data, in real-time or to compel a service provider to collect or record traffic data in real time or cooperate and in the collection or recording of traffic data where the data is required for the purposes of an investigation.
11. Clause 29 of the Bill empowers a police officer or an authorised person to apply to court for an order to permit the collection or recording of the content of any specifically identified electronic

communications or compel a service provider to collect or record or cooperate and assist in the collection or recording of content data, in real-time, of specified communications transmitted by means of a computer system where the data is required for the purposes of an investigation.

12. Clause 30 of the Bill provides for the offences of obstruction of the lawful exercise and misuse of the powers granted under the Bill. The two offences are punishable with a fine not exceeding five million shillings or imprisonment for a term not exceeding three years, or both.
13. Clause 31 of the Bill provides for an avenue of appeal to any person aggrieved by any decision or order made under the Bill within thirty day of the decision or order.
14. Clause 32 of the Bill provides for confidentiality of information provided pursuant to a requirement under the Bill and limits the liability of a service provider for any offence to only willful acts done with its knowledge.
15. Part IV of the Bill is to apply in addition to the provisions of the Mutual Legal Assistance Act, 2011 with specific regard to international cooperation in the investigation and prosecution of computer and cybercrime. It specifically provides for cooperation between the Office of the Attorney General, as the Central Authority established to handle matters of mutual legal assistance, and any requesting State. The Part provides for procedures for the sharing of relevant information, making of requests for preservation or interception of data or information contained in communications and real time collection of traffic data required for the purposes of investigations into computer or cybercrime.
16. Clause 41 of the Bill requires the Office of the Attorney General to ensure that the agency responsible for investigating and prosecuting cybercrime designates a point of contact available on a twenty-four hour, seven-day-a-week basis to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to

computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

17. Part V of the Bill (Clause 42-46) outlines general provisions including territorial jurisdiction for the application of the Bill, power of the Court to order forfeiture of any items seized under the provisions of the Bill and consequential amendments to the Kenya Information and Communications Act, 1998 to repeal sections 83U, 83V, 83W, 83Z, 84A, 84B and 84F. The Part further provides for the power of the Cabinet Secretary to make Regulations.

CHAPTER TWO

PUBLIC PARTICIPATION

2.1 Introduction

18. Pursuant to Article 118(1) (b) of the Constitution and the Standing Order No. 127(3) which provides that the Parliament shall facilitate public participation, the Committee placed an advert in the local dailies on 6th February, 2018 and wrote to the key stakeholders inviting them to submit their views to the Clerk of the National Assembly on or before Tuesday 13th February,2018.

19. By the deadline of submission, the Committee had received thirteen (13) memoranda from the Kenya ICT Action Network (KICTANET); the Media Council of Kenya; the Center for Intellectual Property and Information Technology Law (CIPIT); the Communication Authority of Kenya (CAK); the Kenya Private Sector Alliance (KEPSA); the Information Communication Technology Association of Kenya (ICTAK); SOTE Hub; the Information System Audit and Control Association, Kenya Chapter (ISACA-Kenya); the Technology Service Providers of Kenya (TESPOK); Mr. Michael Otieno; Safaricom Limited; Article 19; and the Ministry of Information, Communication and Technology.

2.2 Committee Meetings

20. Upon receipt of the memoranda, the Committee held thirteen (13) meetings, two (2) of which were held on 23rd and 26th February, 2018 to hear oral submissions from the Ministry of Information Communications and Technology and KICTANET respectively.

2.3 Consideration of the Computer and Cybercrimes Bill, 2017

21. In considering the Computer and Cybercrimes Bill, 2017, the Committee took into account the Memoranda and oral submissions received from the public and its deliberations. The following

constitutes the views of the Committee on the issues arising with regard to each Clause of the Bill—

Clause 2

22. ISACA-Kenya proposed that the Clause be amended to insert definitions for the terms "availability", "confidentiality" and "integrity" as used within the Bill.
23. Mr. Michael Otieno Odhiambo proposed that the Clause be amended to define the scope in which the Cabinet Secretary's Gazette notice with regard to "authorised persons" applies.
24. An unnamed submission proposed that the Clause be amended to define and establish a Cybersecurity Agency or Authority respond to cyber security incidents that threaten Kenyan critical infrastructure and essential service, identify and designate critical information infrastructure and/or establish cyber security codes of practice and standard of performance for implementation by operators of such critical information infrastructure.
25. CIPIT proposed that the Clause be amended to provide a clear explanation of who the law will regard as an "authorised person".
26. ICTAK proposed the insertion of new definitions for the terms "cybersecurity" and "Authority" for purposes of clarity.
27. KEPSA proposed that the Clause be amended in the definition of the term "computer system" to include the aspect of automatic processing of data. They further proposed that the definition of "interception" under the Clause be amended to align it with the definition of "illegal interception" as contained in Article 3 of the Budapest Convention on Cybercrime. It was their additional submission that the Clause be amended to define the term "critical information infrastructure".
28. KICTANET proposed that the Clause be amended to insert definitions for the terms "authorise"; "computer"; "critical infrastructure"; "means of identification"; "film" and "photograph". It was

their further submission that the definitions for the terms "child" and "publish" be moved to the Clause for proper placement.

29. The Committee noted that it would not be prudent to include the definition of words with ordinary meanings in the Clause. In this regard, the Committee agreed with the need to amend the definition of the term "authorised person" and define the term "national critical information infrastructure" for purposes of clarity.

Clause 3

30. In their memorandum, Article 19 proposed the inclusion of protection of human rights in cyberspace as one of the objects of the Bill to take into account the best practices in developing cyber laws. The Committee agreed with this proposal and recommends amendment of the Clause in that regard.

Clause 4

31. Three memoranda received by the Committee contained submissions relating to the Clause. Article 19 sought the inclusion of an "intent to defraud" as a yardstick for determining whether the offence of unauthorized access proposed under the Clause has been committed. CIPIT, on the other hand, noted that subclause (1) may criminalize security research such as penetration testing while KICTANET proposed insertion of an additional subclause to cover handling of data obtained through unauthorized access. The Committee noted that the ingredients of ascertaining whether or not an offence has been committed under the Clause are clearly outlined and that the Clause as drafted prohibits any and all forms of unauthorized access done knowingly. In this regard, penetration testing is done with permission and may not constitute an offence under the Clause.

Clause 5

32. Article 19 sought the deletion of the entire Clause on account of the use of the phrase "under any law" which they argued to be too broad. The Committee disagreed with the submission as the

offence of unauthorized access with intent to commit a further offence proposed in the Clause is an additional offence drawing from the offence of unauthorized access at Clause 4.

Clause 6

33. Two memoranda received by the Committee contained submissions relating to the Clause. Article 19 sought the insertion of an element of "dishonest intention" as an ingredient in the proposed offence of unauthorized interference in subclause (1) and limitation of the scope of the offence to only permanent unauthorized modification at subclause (5). The Committee disagreed with the submission as the Clause clearly outlines sufficient ingredients of the offence of unauthorized interference by requiring the prosecution to prove whether a person has caused unauthorized interference to a computer system program or data intentionally. Further, the clause covers instances of both temporary and permanent modification as both can be equally damaging to the owner of a computer system, program or data.

34. KICTANET sought the deletion and replacement of subclauses (1) and (2) to make the Clause concise and define what interference constitutes under the Clause. The Committee disagreed with this view, noting that the Clause as drafted is clear.

Clause 7

35. Three memoranda received by the Committee contained submissions relating to the Clause. Safaricom sought the deletion of the entire clause for contravening Article 31 of the Constitution on the right to privacy and the provisions of the Kenya Information and Communications Act, 1998 (KICA) and Regulations which prohibit any form of interception in the communications of subscribers. The Committee disagreed with this view as the Clause seeks to prohibit the unauthorized and interception of data and its subsequent transmission to or from a computer system. The Bill allows interception of data where authorized by the Court.

36. ISACA-Kenya sought a reduction of the penalty for the proposed offence of unauthorized interception from a fine not exceeding ten million shillings or imprisonment for a term not exceeding five years to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years. The Committee disagreed with this view as the proposed offence seeks to prohibit conduct with ramifications equal to those contemplated with regard to the proposed offence of unauthorized interference.

37. Article 19 proposed that subclause (2) (c) be amended to limit the scope of injury to only "serious" injury. The Committee disagreed with this view as the inclusion of the word "serious" in subclause (2)(c) would introduce a subjective element to the offence created and lead to challenges of interpretation of the subclause, prosecution of offences and determination of criminal cases.

Clause 8

38. Six memoranda received by the Committee contained submissions relating to the Clause. ISACA-Kenya proposed the reduction of the penalty for disclosing a password from a fine not exceeding five million shillings or imprisonment for a term not exceeding three years to a fine not exceeding one million shillings or imprisonment for a term not exceeding one year as the sharing of passwords is a common occurrence. The Committee disagreed with this view as the Clause clearly limits the application of the penalties proposed to persons who, among other acts, knowing make or receive passwords specifically for the purpose of committing an offence. Subclause (3) outlines adequate exceptions including material used for training, testing or protecting a computer system.

39. Article 19 proposed the deletion of the phrase "without sufficient excuse or justification" appearing in subclause (2) as it contradicts the intent of the subclause. The Committee agreed with this view as no sufficient excuse or justification exists for knowingly receiving or being in

possession of a program, password, device, access code or similar data and intending that it be used to commit or assist in the commission of an offence.

40. CIPIT noted that subclause (1) does not protect the legitimate use of devices and programs that are designed primarily to intercept and capture network traffic. It submitted that he law should not ban such devices or programs in a blanket manner but instead regulate their malicious use.

41. KICTANET sought the amendment of subclause (1) to prohibit the rent or transfer of devices or programmes including such other means of access or control of computers to commit offences. The Committee noted that the Clause as presently drafted sufficiently covers the two proposed scenarios.

42. TESPOK and Safaricom sought the definition of the phrase "illegal device", and the listing of all devices and access codes that may be used in committing offences under the Bill, respectively. The Committee disagreed with these two views as the content of the clause adequately outlines, in principle, what constitutes an illegal device and given the dynamic nature of information and communications technology, it is impossible to exhaustively list all devices that may be used in the commission of an offence under the Bill.

Clause 9

43. The Committee agreed with the content of the clause save for amendments proposed to rectify typographical errors.

Clause 10

44. Three memoranda received by the Committee contained submissions relating to the Clause. ISACA-Kenya sought the deletion of subclause (2) (c) for expanding the scope of a protected system to virtually any computing system. The Committee noted that the subclause (2)(c) defines a computer system used for the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments,

public utilities or public transportation, including government services delivered electronically as a protected system. The subclause therefore sufficiently limits the scope of computer systems targeted.

45. Article 19 proposed amendment of the Clause to provide a narrower and clear definition of phrase "protected computer system" and narrower powers of the Cabinet Secretary to designate protected computer systems under subclause (2) (f). It submitted that subclause (2) as drafted would reduce computer use by the public and grant unlimited powers to the Cabinet Secretary. The Committee Noted that save for paragraph (f) of the subclause, the rest of the contents of subclause (2) outlined specific limits on the scope of the definition of what constitutes a protected system. With regard to paragraph (f), the Committee agreed with the view submitted by Article 19 and recommends that the paragraph be amended to outline the purpose and limits within which the Cabinet Secretary may designate a computer system as a protected computer system.
46. CIPIT noted that it is not clear within the Clause whether all protected computer systems qualify as critical infrastructure. The Committee agreed with this view and recommends a clear definition of the term "critical infrastructure" within the Bill.

Clause 11

47. Three memoranda received by the Committee contained submissions relating to the Clause. ISACA-Kenya sought deletion of a non-existent repetition
48. Article 19 sought deletion of the Clause and amendment of the provisions of the Penal Code relating to espionage. The Committee disagreed with this view as the Clause restricts itself to the technological aspects of espionage.

49. On their part, CIPIT noted that the Bill does not define what a critical infrastructure is. The Committee agreed with this view and noted the need to include a clear definition of the term "critical infrastructure" within the Bill.

Clause 12

50. Six memoranda received by the Committee contained submissions relating to the Clause. Article 19, Media Council of Kenya, ICTAK and CIPIT all proposed the deletion of the entire Clause for infringing on the freedom of expression as guaranteed under Article 33 of the Constitution. Article 19 deemed the phrase "fictitious, false and misleading" as ambiguous and open to abuse by law enforcement officers thus jeopardizing the enjoyment of the freedom of expression. The Media Council of Kenya submitted that the publication of false information has been dealt with under other laws including defamation law.

51. On its part, KICTANET proposed the deletion and replacement of the Clause with a revised text to effectively deal with the issue of "fake news". They submitted that the provision constitutes an unjustifiable limit on the right to freedom of expression and opinion granted under Article 33 of the Constitution and that the revised text should be subjected to the limits to freedom of expression set out at Article 33(2) of the Constitution. The Committee noted that the Clause seeks to limit the freedom of expression especially in light of recent developments in cyberspace and social media where persons share false, fictitious or misleading information with the intent that the information be viewed as authentic and acted upon by the innocent public. The Committee however noted that the Clause fails to express the intention to limit the freedom of expression and the nature and extent of the limitation as required by Article 24(2) of the Constitution. As such, it is necessary to revise the text of the Clause in order to comply with the constitutional requirement.

52. ISACA-Kenya proposed a reduction of the penalty for false publications from a fine not exceeding five million shillings or imprisonment for a term not exceeding two years to a fine not exceeding one million shillings or imprisonment for a term not exceeding one year. It was submitted that the penalty proposed is too prohibitive and may infringe on creativity and restrict the freedom of expression. The Committee did not agree with the view, noting that the fine prescribed under the Bill proposed a maximum penalty that allows the Court discretion on the sentences to impose under the Clause. The Committee noted that, in sentencing convicted persons under the Clause, the maximum penalty allows the Court to consider the nature and severity of each offence as well as its impact on the victims.

Clause 13

53. Six memoranda received by the Committee contained submissions relating to the Clause. ISACA-Kenya, Article 19, Media Council of Kenya, CIPIT and KICTANET sought the deletion of the entire clause arguing that the offence of Child pornography is sufficiently provided for under section 16 of the Sexual Offences Act, 2006. The Committee noted that the Clause and Section 16 of the Sexual Offences Act, 2006 provide for the same offence with differing ingredients and penalties. The Committee therefore noted the need to amend the Sexual Offences Act to harmonize it with the provisions of the Clause.

54. Safaricom Limited proposed widening of the scope of the Clause to include other sexual offences against children such as distribution of adult content to a minor; misleading a minor while engaging them online as well as distribution of content aimed at radicalizing a minor or distributing content likely to spread fear and terror or undermine any rights and privileges that a child is entitled to. The Committee noted that the offences proposed for inclusion are adequately covered under the Sexual Offences Act, 2006 and the Prevention of Terrorism Act, 2011 and that any online element of the offences is adequately covered by Clause 21 of the Bill.

55. TESPOK proposed an amendment to the definition of the term "publish" to exclude the reference to "transmission" arguing that intermediaries are likely to be held responsible for data transmitted through their infrastructure instead of content developers. The Clause would therefore place an onerous financial and technical burden on service providers. The Committee disagree with this view, noting that Clause 32 of the Bill adequately indemnifies service providers. Clause 32(2) provides that a service provider may not be held liable under civil or criminal law for merely providing s service.

Clause 14

56. Two memoranda received by the Committee contained submissions relating to the Clause. Article 19 sought the deletion of the Clause arguing that the offence of computer forgery is adequately provided for under the Penal Code, Cap. 65 of the Laws of Kenya. ISACA-Kenya proposed that the penalties proposed under the Clause be harmonized with the penalties contained in the Penal Code. The Committee noted that the Clause is necessary as its covers the technological elements of forgery and agreed with ISACA-Kenya on the need to harmonize the penalties under the Clause with those under the Penal Code to remove any avenue of the lesser penalty being relied on by an accused person.

Clause 15

57. Two memoranda received by the Committee contained submissions relating to the Clause. KICTANET proposed deletion of the entire clause submitting that fraud is already provided for under numerous sections of the Penal Code and 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. On their part, ISACA-Kenya proposed that the penalty under the Clause be harmonized with the penalties provided under the Penal Code for the offence of fraud. The Committee noted that the Clause is necessary in order to

tackle the technological aspects of fraud. In this regard, the Committee agreed with the submission by ISACA-Kenya on the need to harmonize the penalties under the Clause with those under the Penal Code to remove any avenue of the lesser penalty being relied on by an accused person.

Clause 16

58. Five memoranda received by the Committee contained submissions relating to the Clause. Article 19 sought the deletion of the entire Clause arguing that the offence should be dealt with under other legislation as it is not clear what the phrase "repeated communication in the knowledge that this conduct will cause fear or detrimentally affect a person" means. That the Clause is framed in clear terms which seek to outlaw cyber harassment, an act that is prevalent in the Country today.

59. Safaricom Limited sought the deletion of subclause (3)(a) which outlines a law enforcement defence to the offence of cyberstalking or cyberbullying arguing that it provides an avenue for cyberstalking and cyberbullying. The Committee disagreed with the submission, noting that subclause (3)(c) is a limited defence that applies only to law enforcement agencies. A person advancing the defence under the subclause would have to satisfy the Court that the defence applies to their case.

60. KICTANET and the Media Council of Kenya proposed that the Clause be renamed "Cyber-harassment" and provision be made to allow victims to obtain restraining orders. The Committee agreed with this view, noting that the term "Cyber harassment" covers the two aspects of cyberbullying and cyberstalking and that there is need to allow a victim of cyber harassment to apply for a restraining order pending the determination of a case.

61. ISACA-Kenya proposed a reduction of the penalty under the Clause to a fine not exceeding one million shillings or imprisonment for a term not exceeding one year, arguing that the penalty

proposed under the Clause is too prohibitive. The Committee disagreed with this submission, noting that the issue of cyber harassment has become quite prevalent in the country. It was the view of the Committee that the seriousness of the offence and its potential impact on victims calls for the level of penalties proposed under the Clause to act as a deterrent. .

Clause 17

62. Three memoranda received by the Committee contained submissions relating to the Clause. Article 19, Media Council of Kenya and KICTANET all sought the deletion of the entire Clause arguing that the offence of aiding and abetting in the commission of an offence is adequately provided for under other laws i.e. the Section 20 of the Penal Code Cap. 65. The Committee disagreed with the submissions, noting that the offence of aiding and abetting under the Clause is limited to the offences under the Bill and the Clause is therefore a necessary inclusion in the Bill.

Clause 18

63. Two memoranda received by the Committee contained submissions relating to the Clause. KEPSA and KICTANET memoranda proposed that subclause (1)(b) be reworded to align it with the requirements of Article 50(2) of the Constitution on the right to a fair hearing, and for purposes of clarity, respectively. The Committee disagreed with the two submissions on the Clause, noting that the contents of the clause are clear as it deems offences upon corporations and its principal officers and prescribes penalties that only apply upon conviction of the officers charged.

Clause 19

64. The Committee agreed with the provisions of Clause 19. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 20

65. The Committee agreed with the provisions of Clause 20. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 21

66. Two memoranda received by the Committee contained submissions relating to the Clause. Article 19 sought the deletion of the entire Clause arguing that the Clause will discourage computer use and thus work against the public interest. On the other hand, KICTANET sought deletion and replacement of the Clause with a one that a provides criteria for aggravating factors to be considered when charges or sentences are enhanced for offences committed through use of a computer system. The Committee disagreed with the submission by Article 19, noting that the Clause is a necessary inclusion in the Bill to cater for instances where ordinary offences are committed through the use of computer technology. The Committee agreed with the submission by KICTANET proposing that the clause deem the use of computer technology to commit offences covered under other laws as constituting an aggravated offence with a penalty similar to the penalty set out in the law governing the initial offence. In this regard, the Committee therefore noted the need to amend the Clause.

Clause 22

67. KEPSA proposed deletion of subclause (3) arguing that the subclause gives a blanket approval for the officers of the National Intelligence Service and the Kenya Defence Forces who are not envisaged to be the authorized personnel. The Committee disagreed with this submission, noting that subclause (3) only states that the powers under the Bill do not reduce any other powers granted to investigate agencies under the National Intelligence Serve Act, the Kenya Defencc Forces Act and the National Police Service Act. The subclause does not, contrary to the assertion in the submission, designate officers of the National Intelligence Service or the Kenya Defence Forces as authorised persons under the Bill.

Clause 23

68. Four memoranda received by the Committee contained submissions relating to the Clause. TESPOK proposed definition of the term "authorised person" to mean a police officer

specifically designated to handle cybersecurity in order to provide clarity. They further proposed a definition for the term "stored data". The Committee did not agree with the submission, noting that the definition proposed for the term "authorised person' would unduly restrict the persons that may be authorised to conduct investigations under the Bill, including cyber and forensic experts. Further, the Committee noted that the term "stored data" is self-explanatory and therefore does not require further definition under the Bill.

69. Safaricom Limited proposed amendment of subclauses (1) (b) and (3) to require that any access, search or seizure of data under the Clause be conducted with the assistance of a principal officer or person acting in a similar capacity. This, in their view, would ensure that the daily business operations of the entity being searched are not compromised. The Committee disagreed with the proposal, noting that its inclusion as a requirement under the Clause would hamper execution of a validly obtained search warrant where the proposed "principal officer or person acting in a similar capacity" is unavailable is or uncooperative.

70. Michael Otieno Odhiambo proposed amendment of the Clause to ensure that access to data or an application program only done in the presence of an employee of the entity responsible for the data and with the knowledge of an employee that is responsible for the data in order safeguard the integrity of the data or the operations of the application or program. He additionally proposed that—

    (a) the Clause be amended to require the investigating authority to ensure confidentiality of the data accessed from the premises of interest;

    (b) subclause (4) be amended to require that where a police officer or the investigating authority needs to extend a search to other systems, the officer or authority should

officially notify the owner of the data or application program of the intended extension of their search and, in the absence of a Court warrant, seek authority for the exercise; and

(c) subclause (5) be amended to provide for the consequences where data is used for purposes other than the intended reason it was obtained in order to provide a deterrent.

71. The Committee agreed with some of Mr. Odhiambo's submission on the need for the Bill to require investigating authorities to maintain the integrity and confidentiality of information seized while executing a search warrant. On issue of the presence of an employee being searched, the Committee noted that requiring the presence of the employee would unduly hamper the execution of a valid warrant. It was the view of the Committee that the Clause expressly requires investigating authorities to obtain a warrant outlining the extent of their search and seizure. In that regard, it follows that where the investigating authorities propose to extend their search, they have to obtain permission from the Courts, unless the affected person or entity consents to such an extension.

72. KEPSA sought deletion and replacement of the word "may" in subclause (1) with the word "shall" in order to make it mandatory for investigative agencies to obtain a court order under the Clause. The Committee disagreed with this view, noting that the term "may" as used in the Clause, adequately makes it mandatory for the police or authorised persons to obtain a warrant from the Court before conducting a search or a seizure under the Bill.

Clause 24

73. Eleven Memoranda received by the Committee contained submissions relating to the Clause. ISACA-Kenya, Article 19, TESPOK, ICTAK, Michael Otieno Odhiambo, KEPSA, KICTANET of the memoranda sought the deletion of the Clause arguing that there is no justification to conduct a search without a warrant and that the provision contradicts Article 24(2) and 31 of the Constitution. It was further submitted that the sections of the Criminal Procedure Code, Cap. 75

of the Laws of Kenya referenced in the Clause with regard to conducting a search without a warrant do not exist.

74. TESPOK, CAK, the Ministry of Information, Communications and Technology, CIPIT, Safaricom Limited and KEPSA proposed that the Clause be amended to outline the special circumstances in which a search could be conducted without a warrant. It was submitted that special circumstances could include instances where the crimes being committed are of a nature that does not allow investigative agencies enough time to apply for a warrant e.g. kidnapping and Terrorism. The Committee noted that there exists no justification to conduct a search without warrant. The Provision, additionally, contradicts Article 24(2) of the Constitution. The Committee agreed with the view to delete the Clause noting that it overly infringes on the right to privacy as enshrined in the Constitution.

75. **Clause 25**

The Committee agreed with the provisions of Clause 25. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 26

76. Nine memoranda received by the Committee contained submissions relating to the Clause. KEPSA sought the amendment of subclause (1) to delete the word "may" and replace it with the word "shall" to require the investigatory authorities to obtain a production order from Court. The Committee disagreed with this view, noting that the term "may" as used in the Clause, adequately makes it mandatory for the police or authorised persons to obtain a production order from the Court before requiring the production of data or subscriber information for the purposes of investigations.

77. Safaricom Limited sought the deletion of subclause (4) which allows the Court to require that the existence of a production order be kept confidential, arguing that the subclause is in conflict with

80. The Committee agreed with the two submissions, noting that subclause (2) does not provide a definite period in the notice for preservation and partial disclosure of traffic data, a gap that may be abused to the disadvantage of affected citizens. The Committee agreed that a thirty-day period for the initial notice is sufficient as subclause (3) allows the investigating agencies to apply for an extension of the period that the traffic data is to be preserved. Further, the Committee noted that the disclosure of the existence of an order issued under the Clause is not likely to compromise any ongoing investigations. The Committee agreed with the proposal to delete subclause (4).

Clause 28

81. Seven memoranda received by the Committee contained submissions relating to the Clause. Article 19 sought the deletion of the entire Clause arguing that the extended surveillance periods provided for contravene international law and best practices. The Committee disagreed with this view noting that the inclusion of the Clause is necessary in order to allow investigating agencies court-mandated real time access to traffic data to assist them to monitor and prevent the commission of cybercrimes.

82. ISACA-Kenya and KICTANET proposed that subclause (4) be amended to reduce the period within which real time collection of traffic data may be allowed from a maximum of six months to a maximum of three months or one month, respectively, as preservation of real-time data is an expensive exercise. The Committee disagreed with this view, noting that the six-month period provided under the Clause for real-time collection or recording of data is reasonable as the complexity of the investigations conducted under the Bill may vary. In any event, the Committee noted that the period under subclause (4) is the upper limit of what the Court is granted discretion to allow depending on the circumstances of each investigation.

83. Safaricom Limited proposed amendment of subclauses (1)(a) and (3) to require that any collection or recording of traffic data be conducted with the assistance of a principal officer or person acting in a similar capacity in order to prevent disruption of the daily business operations of entities affected by the provision. Additionally, one memorandum proposed the inclusion of a definition of the term "stored data". The Committee disagreed with the proposal, noting that its inclusion as a requirement under the Clause would hamper execution of a validly obtained Court order in the event the proposed "principal officer or person acting in a similar capacity" is unavailable or uncooperative.

84. CIPIT noted that Kenya's existing surveillance legislation only permits intelligence agents and police officers the rank of Chief Inspector and above to apply for a warrant of the type covered under the Clause and that the clause therefore expands the scope of investigatory powers to undertake very intrusive surveillance. The Committee agreed with this view and noted the need to amend the Bill to limit the persons authorised to apply for Court orders or search warrants to persons above the rank of Chief Inspector of Police in order to prevent abuse of the powers granted under the Bill by investigative agencies.

85. KEPSA proposed amendment of subclause (1) to delete the word "may" and replace it with the word "shall" to require the investigatory authorities to obtain an order for real-time collection of data from Court. The Committee disagreed with this view, noting that the term "may" as used in the Clause adequately makes it mandatory for the police or authorised persons to obtain an order from the Court before requiring the real time collection or recording of traffic data for the purposes of investigations.

Clause 29

86. Six memoranda received by the Committee contained submissions relating to the Clause. Article 19, TESPOK and KICTANET memoranda sought the deletion of the entire Clause arguing that

the clause contravenes Article 31 of the Constitution on the right to privacy, the extended surveillance periods provided for contravene international law and best practices; and that the Clause may expose service providers to litigious matters, respectively. The Committee disagreed with these views noting that the Clause is a necessary inclusion in the Bill which allows the police or authorised persons court-mandated real-time access to the content data of communications to assist them in the monitoring and prevention of cybercrime. With regard to the issue of the liability of service providers, the Committee noted that Clause 32 of the Bill outlines an adequate protection for the good-faith actions of service providers and their compliance with valid orders issued by the Court under the provisions of the Bill.

87. Safaricom Limited sought the deletion of subclauses (1)(b), (6) and (7) arguing that the subclauses contravene Article 31 of the Constitution on the right to privacy, contravene the obligations of service providers under KICA to inform subscribers on information being collected about them, and expose service providers to litigation, respectively. The Committee disagreed with these views noting that subclause (1) provides an adequate safeguard against arbitrary violation of the right to privacy by requiring investigating agencies to first obtain a Court order for which they must give reasons. As the clause relates to the collection of real-time content data, the Committee noted that subclause (6) is a necessary inclusion in order to maintain the confidentiality of ongoing investigations.

88. KEPSA proposed amendment of subclause (1) to delete the word "may" and replace it with the word "shall" to require the investigatory authorities to obtain an order to collect or compel a service provider to disclose real-time traffic data transmitted by means of a computer system from the Court. The Committee disagreed with this view, noting that the term "may" as used in the Clause adequately makes it mandatory for the police or authorised persons to obtain an order

from the Court before seeking the real time collection or recording of content data for the purposes of investigations.

Clause 30

89. The Committee agreed with the provisions of Clause 30. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 31

90. The Committee agreed with the provisions of Clause 31. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 32

91. KEPSA proposed deletion and replacement of the Clause with a revised text in order to protect intermediaries from liability for content generated by their users. The Committee disagreed with the proposal, noting that the Clause as drafted adequately covers the issue of protecting service providers from incurring any liability as a result of complying with orders issued by the Court under the provisions of the Bill.

Clause 33

92. The Committee agreed with the provisions of Clause 33. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 34

93. CIPIT noted the need for judicial oversight in the spontaneous forwarding of information under the Clause. The Committee disagreed with this view noting that the Clause related to the spontaneous sharing of information with friendly countries hence dispensing with the need to seek input from the Courts.

Clause 35

94. The Committee agreed with the provisions of Clause 35. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 36

95. The Committee agreed with the provisions of Clause 36. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 37

96. The Committee agreed with the provisions of Clause 37. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 38

97. Three memoranda received by the Committee contained submissions relating to the Clause. Article 19 sought the deletion of the entire Clause arguing that the use of the phrase "without authorization" leaves the Clause open to abuse and allows disproportionate hacking. Similarly, Mr. Michael Otieno Odhiambo proposed that the Clause be considered for amendment for posing an implementation challenge as the data privacy laws of most countries where data is resident for cloud-hosted solutions may require explicit authorization prior to access. It was his submission that it may not be feasible to expect access without authorization. The Committee agreed with the two proposals to the extent that the Clause contains an inherent contradiction with the inclusion of the phrase "without authorisation". The Committee therefore noted the need to delete the phrase in order to cure the contradiction.

98. On their part, KICTANET proposed deletion of the phrase "(open source)" used in the Clause. The Committee agreed with this view, noting that the deletion of the phrase would enhance the clarity of the Clause.

Clause 39

99. The Committee agreed with the provisions of Clause 39 save for the need to correct a typographical error at subclause (2)(g). As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 40

100. The Committee agreed with the provisions of Clause 40. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 41

101. Two memoranda received by the Committee contained submissions relating to the Clause. Both CAK and the Ministry of Information, Communications and Technology proposed amendment of subclause (1) to delete the phrase "and prosecuting crime" to create the distinction between investigatory and prosecutorial roles under the Bill. The Committee agreed with this view, noting that the Central Authority established under the Bill falls under the purview of the Office of the Attorney General who does not have prosecutorial powers under the Constitution. it would therefore be necessary to delete the reference prosecution in the Clause.

Clause 42

102. The Committee agreed with the provisions of Clause 42. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 43

103. The Committee agreed with the provisions of Clause 43. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 44

104. The Committee agreed with the provisions of Clause 44. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 45

105. The Committee agreed with the provisions of Clause 45. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause.

Clause 46

106. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Clause. In its deliberation, the Committee noted the need to amend

the Clause in compliance with the provisions of Article 94(6) of the Constitution which requires an an Act of Parliament that delegates legislative powers to expressly specify the purpose and objectives for which that authority is conferred, the limits of the authority, the nature and scope of the law that may be made, and the principles and standards applicable to the law made under the authority.

Schedule

107. The Committee agreed with the Schedule. As at the time of concluding its report, the Committee had not received any memoranda with submissions relating to the Schedule.

Additional proposals

108. Six memoranda received by the Committee contained submissions on additional proposals not covered under the Bill. These proposals include—

(a) Establishing a governance council to provide guidance training and overall implementation of the Act once passed;

(b) Establishing a National Cybersecurity Authority of Kenya for coordinated administration management and governance on cybersecurity matters in Kenya;

(c) Insertion of new offences covering terrorism related activities on the internet; money laundering through the internet; deportation of foreigners convicted of cybercrimes; insult to religion; issuing of threats, blackmail or incitement through the internet; and identity theft for purposes of internet fraud;

(d) Insertion of references to the Extradition (Contiguous and Foreign Countries) Act wherever the Bill refers to the Mutual Legal Assistance Act;

(e) Insertion of a new Clause requiring Cabinet Secretary responsible for National Security develop Standard Operating Procedures and Guidelines for the conduct, search, seizure and collection of electronic evidence;

(f) Insertion of a new clause on the limitation of the right to privacy by the Bill;

(g) Insertion of a new Clause on the limitation of the right to privacy by the Bill;

(h) Insertion of a new Clause on online grooming;

(i) Insertion of a new Clause on child sex tourism;.

(j) Insertion of a new Clause on Identity theft;

(k) Insertion of a new Clause on Cyber Squatting;

(l) Insertion of a new Clause on disclosure of a private photograph or film;

(m) Insertion of a new Clause on Social engineering attacks;

(n) Insertion of a new Clause placing reporting obligations on the Director of Public Prosecutions in relation to investigations and prosecutions taken under the Bill;

(o) Insertion of a new Clause on duties of persons collecting Personal data;

(p) Insertion of a new Clause on unlawful obtaining and disclosure of personal data;

(q) Insertion of a new Clause to require the Cabinet Secretary to develop a framework to safeguard the security of personal data;

(r) Insertion of a new Clause on the liability of legal person under the Bill;

(s) Insertion of a new Clause establishing a National Cybersecurity Council;

(t) Insertion of a new Clause on the functions of the Communications Authority in relation to cybersecurity;

(u) Insertion of a new Clause on the functions of the National Kenya Computer Incident Response Team Coordination Center;

(v) Insertion of a new Clause on the functions of the Cybercrime Unit; and

(w) Insertion of a new Clause on reporting of cyber risks by corporate entities.

The Committee noted that there would be need to amend the Bill to include the offences of Cyber squatting, Wrongful distribution of intimate images, Phishing, Interception of electronic messages or money transfers, Willful misdirection of electronic messages and online grooming of a child.

CHAPTER THREE

COMMITTEE RECOMMENDATIONS

109. In light of the submissions in the Memoranda, the oral representations made before the Committee and the Committee deliberations on the Bill, the Committee recommends—

CLAUSE 2

THAT, Clause 2 of the Bill be amended—

(a) by deleting the definition of "authorised person" and substituting therefor the following new definition—

~~"authorised person" means an officer in a law enforcement agency or a cybersecurity expert~~ designated by the Cabinet Secretary responsible for matters relating to national security by notice in the *Gazette* for the purposes of Part III of this

(b) by deleting the definition of "Authority" and substituting therefor the following new definition—

""Authority" means the Communications Authority of Kenya";

(c) by deleting the definition of "Central Authority" and substituting therefor the following new definition—

""Central Authority" means the Office of the Attorney General";

(d) in the definition of "premises" by inserting the words "a physical or virtual space in which data is maintained, managed, backed up remotely and made available to users over a network" immediately after the word "aircraft";

(e) by deleting the definition of "requested state" and substituting therefor the following new definition—

""requested state" means a state being requested to provide legal assistance under the terms of this Act";

(f) by deleting the definition of "requesting state" and substituting therefor the following new definition—

""requesting state" means a state requesting for legal assistance and may for the purposes of this Act include an international entity to which Kenya is obligated";

(g) by inserting the following new definitions in the proper alphabetical sequence—

"national critical information infrastructure" means a vital virtual system and asset whose incapacity, destruction or modification would have a debilitating impact on the security, economy, public health or safety of the country;

Justification: For the purpose of clarity.

CLAUSE 3

THAT, clause 3 of the Bill be amended—

(a) by deleting paragraph (c) and substituting therefor the following new paragraph—

"(c) facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes";

(b) in paragraph (c) by inserting the following new paragraph immediately after paragraph (c)—

"(ca) protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution;"

Justification: To include the facilitation, prevention, detection and punishment of cybercrime and the protection of the human rights in cyberspace as part of the objects of the Bill.

CLAUSE 5

THAT, clause 5 of the Bill be amended in subclause (2) by deleting the word "this" appearing immediately after the words "purposes of";

Justification: To ensure consistency and clarity of the Clause

CLAUSE 7

THAT, clause 7 of the Bill be amended in subclause (2) by deleting the word "of" appearing immediately after the words "for a term" at the end of the subclause;

Justification: To rectify typographical errors

CLAUSE 8

THAT, clause 8 of the Bill be amended—

(a) in subclause (2) by deleting the words "without sufficient excuse or justification" appearing immediately after the words "this Part";

(b) in subclause (3) by deleting the words "in thereof" appearing immediately after the word "described" and substituting therefor the words "under the subsections";

Justification: The phrase "without sufficient excuse or justification" contradicts the intent of subclause (2). No sufficient excuse or justification exists for knowingly receiving or being possession of a program, password, device, access code or similar data and intending that it be used to commit or assist in the commission of an offence.

CLAUSE 9

THAT, clause 9 of the Bill be amended in subclause (1) by deleting the word "term" appearing immediately after the word "imprisonment";

Justification

To rectify a typographical error.

CLAUSE 10

THAT, clause 10 of the Bill be amended—

(a) in subclause (1) by inserting the words "for a" immediately after the word "imprisonment"

(b) in subclause (2)(f) by deleting the words "by the Cabinet Secretary in the manner or form as the Cabinet Secretary may consider appropriate" and substituting therefor the words—

"relating to the security, defence or international relations of Kenya, critical information, communications, business or transport infrastructure and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication and technology."

Justification:

(i) To correct a typographical error; and

(ii) To prescribe the purposes for which the Cabinet Secretary may designate a system to be a protected system under the Bill.

CLAUSE 11

THAT, clause 11 of the Bill be amended in subclause (3) by inserting the word "shillings" immediately after the words "five million";

Justification: To rectify a typographical error.

CLAUSE 12

THAT, clause 12 of the Bill be amended by—

(a) renumbering the existing provision as subclause (1);

(b) inserting the following new subclause immediately after subclause (1)—

"(2) Pursuant to Article 24 of the Constitution, the freedom of expression under Article 33 of the Constitution shall be limited in respect of the intentional publication of false, misleading or fictitious data or misinformation that—

(a) is likely to—

(i) propagate war; or

(ii) incite persons to violence;

(b) constitutes hate speech;

(c) advocates hatred that—

(i) constitutes ethnic incitement, vilification of others or incitement to cause harm; or

(ii) is based on any ground of discrimination specified or contemplated in Article 27(4) of the Constitution; or

(d) negatively affects the rights or reputations of others.

Justification: To provide the extent of limitation of the freedom of expression as required by Article 24(2) of the Constitution..

CLAUSE 13

THAT, clause 13 of the Bill be deleted;

Justification: To transfer the proposals under the clause to a harmonized amendment to the Sexual Offences Act, 2011.

CLAUSE 16

THAT, clause 16 of the Bill be amended—

(a) by deleting the marginal note and substituting therefor the following marginal note—

"cyber harassment";

(b) in subclause (1) by deleting the words "and repeatedly" appearing in the opening statement;

(c) by inserting the following new subclauses immediately after subclause (3)—

"(4) A person may apply to Court for an order compelling a person charged with an offence under subclause (1) to refrain from—

(a) engaging or attempting to engage in; or

(b) enlisting the help of another person to engage in,

any communication complained of under subsection (1);

(5) The Court—

(a) may grant an interim order; and

(b) shall hear and determine an application under subsection (4) within fourteen days.

(6) An intermediary may apply for the order under subsection (4) on behalf of a complainant under this section.

(7) A person may apply for an order under this section outside court working hours.

(8) The Court may order a service provider to provide any subscriber information in its possession for the purpose of identifying a person whose conduct is complained of under this section.

(9) A person who contravenes an order made under this section commits an offence and is liable, on conviction to a fine not exceeding one million shillings or to imprisonment for a term not exceeding six months, or to both.

Justification: Cyber harassment covers the two aspects of cyber bullying and cyber stalking. The amendment also allows for a victim to apply for a restraining order.

NEW CLAUSES

THAT, the Bill be amended by inserting the following new clauses immediately after clause 16—

Cybersquatting

16A. A person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right, commits an offence and is liable on conviction to a fine not exceeding two Million shillings or imprisonment for a term not exceeding two years or both.

Wrongful distribution of intimate images.

16B. A person who transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate image of another person commits an offence and 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.

Identity theft and impersonation.

16C. A person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine not exceeding three million d shillings or to imprisonment for a term not exceeding three years or both.

Phishing.

16D. A person who creates or operates a website or sends a message through a computer system with the intention to induce the user of a website or the recipient

of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system, commits an offence and is liable upon conviction to a fine not exceeding three million shillings or to imprisonment for a term not exceeding three years or both.

Interception of electronic messages or money transfers.

16E. A person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed commits an offence and is liable on conviction to a fine not exceeding ten million shillings or to a term of imprisonment not exceeding seven years or both.

Willful misdirection of electronic messages.

16F. A person who willfully misdirects electronic messages commits an offence and is liable on conviction to a fine not exceeding one million shillings or to imprisonment for a term not exceeding one year or both.

Justification:

To include the offences of cyber squatting, wrongful distribution of intimate images, phishing, interception of electronic messages or money transfers, and willful misdirection of electronic messages as offences under the Bill.

CLAUSE 21

THAT, the Bill be amended by deleting clause 21 and substituting therefor the following new Clause—

Additional penalty for other offences committed through use of a computer system.

21. (1) A person who commits an offence under any other law through the use of a computer system commits an offence and shall be liable on conviction to a penalty similar to the penalty provided under that law.

(2) A Court shall, in determining whether to sentence a person convicted of an offence under this section, consider—

(a) the manner in which the use of a computer system enhanced the impact of the offence;

(b) whether the offence resulted in a

commercial advantage or financial gain;

(c) the value involved, whether of the consequential loss or damage caused, or the profit gained from commission of the offence through the use of a computer system;

(d) whether there was a breach of trust or responsibility;

(e) the number of victims or persons affected by the offence;

(f) the conduct of the accused; and

(g) any other matter that the court deems fit to consider.

Justification: To make the use of computer technology to commit offences covered under other laws as constituting an aggravated offence with a penalty similar to the penalty set out in the law governing the initial offence. Under the revised clause, the Court will have a discretion to consider the circumstances of each case before applying the enhanced sentence.

CLAUSE 23

THAT, clause 23 of the Bill be amended—

(a) in subclause (7) by inserting the following new paragraphs immediately after paragraph (b)—

"(c) maintain the integrity of a computer system, any data or information accessed or retained; and

(d) maintain the confidentiality of a computer system, any data or information accessed during the execution of the warrant."

(b) in sub clause (8) by deleting paragraph (b) and substituting therefor the following new paragraph—

"(b) compromises the integrity or confidentiality of a computer system, data or information accessed or retained under this section or misuses the powers granted under this section,

commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both."

Justification: To require investigating authorities to maintain integrity and confidentiality of information seized while executing a search warrant.

CLAUSE 24

THAT, Clause 24 be deleted

Justification: There exists no justification to conduct a search without a warrant. The provision, additionally, contradicts Article 24(2) and 31 of the Constitution.

CLAUSE 26

THAT, clause 26 of the Bill be amended by—

(a) deleting subclause (4);

Justification: The requirement to maintain confidentiality of the existence of an order under the clause is not necessary.

(b) deleting subclause (6);

Justification: The clause violates the right to privacy. The police or the authorized persons under the Act should seek permission from the Court before compelling the production of data or subscriber information.

CLAUSE 27

THAT, clause 27 of the Bill be amended—

(a) in subclause (2) by deleting the words "the period specified in the notice" and substituting therefor the words "thirty days"

Justification: To define time limit for preservation of traffic data.

(b) by deleting subclause (4);

Justification: The requirement to maintain confidentiality of the existence of an order under the clause is not necessary.

CLAUSE 28

THAT, clause 28 of the Bill be amended

(a) in subclause (4) by deleting the word "not" appearing immediately after the words "for a period";

(b) in subclause (7) by inserting the word "shillings" immediately after the words "ten million" appearing in paragraph (a);

Justification: To rectify a typographical errors

CLAUSE 29

THAT, clause 29 of the Bill be amended—

(a) in subclause (1) by deleting the words "a serious" appearing immediately after the words "in respect of" in the opening statement and substituting therefor the words "an";

(b) in subclause (7)(a) by inserting the word "shillings" immediately after the words "ten million";

Justification: To delete a subjective reference and to rectify a typographical error.

CLAUSE 33

THAT, clause 33 of the Bill be amended—

(a) in subclause (1) by inserting the words " the Extradition (Contiguous and Foreign Countries) Act" immediately after the phrase "2011".

(b) in subclause (4) by inserting the words " the Extradition (Contiguous and Foreign Countries) Act" immediately after the phrase "2011".

Justification: To include a reference to the Extradition (Contigous and Foreign Countries Act). The two Acts are complimentary in ensuring successful prosecution of offences under the Bill.

CLAUSE 38

THAT, clause 38 of the Bill be amended by deleting—

(a) the word "another" wherever it appears;

Justification: to rectify a typographical error.

(b) the words "without the authorisation but" appearing immediately after the word "may" in the opening statement;

Justification: the phrase contradict the intent of the clause.

(c) the phrase "(open source)" appearing in paragraph (a);

Justification: to enhance the clarity of the clause.

CLAUSE 39

THAT, clause 39 of the Bill be amended in subclause (2)(g) by inserting the words "to the" immediately after the word "relevant";

Justification: to correct a typographical error.

CLAUSE 41

THAT, clause 41 of the Bill be amended in subclause (1) by deleting the words "and prosecuting" appearing immediately after the word "investigating".

Justification: The Central Authority established under ether Bill falls under the purview of the Office of the Attorney General who does not have the prosecutorial powers under the Constitution.

CLAUSE 46

THAT, the Bill be amended by deleting Clause 46 and substituting therefor the following new clause—

PART VI—PROVISIONS ON DELEGATED POWERS

Regulations.

46. (1) The Cabinet Secretary may make regulations generally for the better carrying into effect of any provisions under this Act.

(2) Without prejudice to the foregoing, regulations made under this section may provide for standard operating procedures for the conduct, search, seizure and collection of electronic evidence.

(3) For the purposes of Article 94 (6) of the Constitution—

(a) the purpose and objective of delegation under this section is to enable the Cabinet Secretary to make regulations to provide for the better carrying into effect of the provisions of this Act and to enable the Authority to discharge its functions more effectively;

(b) the authority of the Cabinet Secretary to make regulations under this Act will be limited to bringing into effect the provisions of this Act and to fulfil the objectives specified under this section;

(c) the principles and standards applicable to the regulations made under this section are those set out in the Interpretation and General Provisions Act and the Statutory Instruments Act, 2013.

Cap 2,
No. 23 of 2013

Justification: To comply with the provisions of Article 94(6) of the Constitution;

SCHEDULE

THAT, the Schedule to the Bill be amended by inserting the following amendments to the Sexual Offences Act—

The Sexual offences Act be amended by—

(a) deleting Section 16 and substituting therefor the following new section—

16. Child pornography

(1) A person, including a juristic person, who knowingly—

(a) possesses an indecent photograph of a child;

(b) displays, shows, exposes or exhibits obscene images, words or sounds by means of print, audio-visual or any other media to a child with intention of encouraging or enabling a child to engage in a sexual act;

(c) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his or her possession an indecent photograph of a child;

(d) imports, exports or conveys any obscene object for any of the purposes specified in subsection (1), or knowingly or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation;

(e) takes part in or receives profits from any business in the course of which he or she knows or has reason to believe that obscene objects are, for any of the purposes specifically in this section, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation;

(f) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be produced from or through any person; or

(g) offers or attempts to do any act which is an offence under this section,

commits an offence and is liable upon conviction to imprisonment for a term of not less than six years or to a fine of not less than five hundred thousand shillings or to both and upon subsequent conviction, to imprisonment to a term of not less than seven years without the option of a fine.

(2) This section shall not apply to—

(a) Publication or possession of an indecent photograph where it is proved that such publication or possession was intended for bona fide scientific research, medical, religious or law enforcement purpose; the indecent representation of a child in a sculpture, engraving, painting or other medium on or in any ancient monument recognised by law; and

(b) activities between two persons above eighteen years of age by mutual consent.

(3) For the purposes of subsection (1),—

(a) an image is obscene if—

(i) it is lascivious or appeals to prurient interest; or

(ii) its effect, or where it comprises two or more distinct items, the effect of any one of its items, if taken as a whole, tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(b) an indecent photograph includes a visual, audio or audio visual representation depicting—

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; or realistic images representing a child engaged in sexual activity.

(b) inserting the following new section immediately after section 16—

Sexual communication with a child

16A. (1) A person of eighteen years and above who knowingly communicates with a child in—

(i) a sexual manner; or

(ii) a manner intended to encourage the child to communicate in a sexual manner,

commits an offence and is liable, on conviction, to a fine of not less than five hundred thousand shillings or imprisonment for a term of not less than five years, to both.

(2) For the purposes of this section, a communication is sexual if—

(a) any part of it relates to sexual activity, or

(b) a reasonable person would consider any part of the communication to be sexual.

Justification:

(i) To amend section 16 of the Sexual Offences Act, 2011 to harmonize its provisions with the provisions of the deleted clause 13; and

(ii) To provide for the offence of sexual communication with a child (grooming) in the Sexual Offences Act, 2011.

THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATIONAND INNOVATION

MEMBERS ATTENDANCE LIST

Adoption of the Report on Computer and CyberCrimes Bill, 2017 on 19th March, 2018 at 2.00pm on 5th floor Continetal House,Parliament Buildings.

NO.	NAME	SIGNATURE
1.	Hon. Kisang, William Kipkemoi, M.P - **Chairperson**	
2.	Hon.George, Macharia Kariuki, M.P - **Vice – Chairperson**	
3.	Hon.Liza, Chelule Chepkorir, M.P.	
4.	Hon.Alfah, O. Miruka, M.P.	
5.	Hon. Annie Wanjiku Kibeh, M.P.	
6.	Hon. Joshua Kimilu, Kivinda, M.P.	
7.	Hon.Marwa Kitayama Maisori, M.P.	
8.	Hon.Mwambu Mabongah, M.P.	
9.	Hon.Maritim Sylvanus, M.P.	
10.	Hon.Mwangaza Kawira, M.P.	
11.	Hon. Jonah Mburu, M.P.	
12.	Hon. Gertrude Mbeyu Mwanyanje,M.P	
13.	Hon.Wamuchomba, Gathoni, M.P.	
14.	Hon.(Eng).Mark Nyamita Ogola,M.P	
15.	Hon. John Kiarie Waweru, M.P.	
16.	Hon. Erastus Nzioka Kivasu, M.P.	
17.	Hon. Innocent Momanyi, Obiri, M.P.	
18.	Hon. Godfrey Osotsi, Atieno , M.P.	
19.	Hon.Anthony, Tom Oluoch, M.P.	

War on the girl-child: Kuria is one of the regions in Kenya with the highest number of school dropouts

Where stigma drives married women to FGM

Elders believed to have magical powers that can bring problems to those who are uncircumcised

BY VIVERE NANDIEMO
ndiemo@yahoo.com

Ms Robi Nchagwa is 40 but used to feel like an outcast until four years ago. She was labelled a bad omen in her Nyamagongwi village, Kuria East Sub-County.

Her husband's relatives disliked her and blamed her for the misfortunes that befell them.

All this because she had refused to be circumcised as a girl.

In a community where girls must face the knife, it was unheard of.

"I was seen as a pariah. My husband's relatives blamed me for the misfortunes that befell the family," she said.

According to Kuria traditions, an uncircumcised woman should not be married. Any man who marries such a woman attracts problems.

The uncut woman — derogatorily called "*irikunene*" — is not allowed to mingle with others, especially at social functions.

Ten years into her marriage, Nchagwa could take it no longer. She gave in to pressure and went for the cut in 2014.

"I was tired of being mistreated and my husband was almost marrying a second wife. I had to do it and I am now at peace with everyone though I feel it was not right," Ms Nchagwa said.

As the world marks the International Day on Zero Tolerance for FGM, campaigners say stigma is one of the main challenges in the battle against the cut.

Ms Vera Robi, the founder of Kuria Anti-FGM and Centre for Child Empowerment, said many married women were being forced into the rite.

> I was seen as a pariah. My husband's relatives blamed me for the misfortunes that befell the family. I had to do it and I am now at peace with everyone though I feel it was not right."
> Robi Nchagwa

"Girls fear being subjected to the same situation in future and opt for the cut," Ms Robi said.

Apart from the stigma, the community still holds on to beliefs and taboos that protect FGM. Elders wield enormous influence.

It is believed that those who reject the rite are bound to face serious consequences from Eresa, the god of circumcision.

According to the belief, mysterious deaths, accidents, strange illnesses, unstable marriages, insanity and other misfortunes follow such people.

Mr Ng'ariba Mwita, an elder, said many deaths and family break-ups were linked to opposition to the cut.

"These cases are real. Those who disobey the ancestors face consequences," he told the *Nation*.

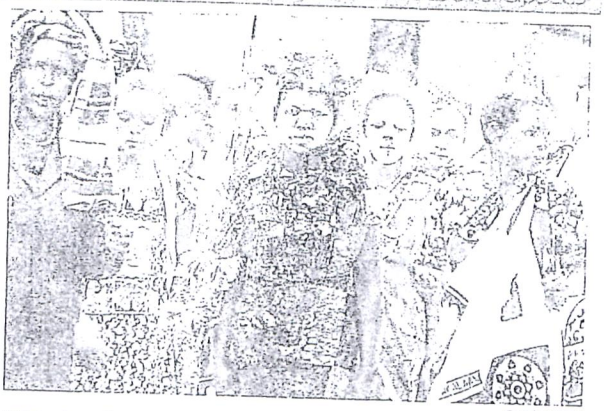
It is believed elders have special powers from Eresa to perform magical feats known as 'tambiko' to cast a spell on anyone who does not go for the cut.

Deputy County Commissioner Wesley Koech admits that the beliefs have slowed the government's efforts in combating FGM.

"The beliefs are strong. Elders threaten those who are opposed to them," Mr Koech said.

However, he maintained that the government would not relent in the war against FGM.

FGM is linked to the high number of school dropouts and teenage pregnancies in Kuria.



FILE | NATION

Initiates leave the compound of the *omosari* — the circumciser — in Kuria East Sub-County. The International Day on Zero Tolerance for FGM is being observed today.

BRIEFLY

NYERI

Doctor denies running medical college illeg

Embu Level Five Hospital (Moses Njue has been freed or Sh200,000 bond after denying op erating a college illegally. Dr Njue also denied admitting student Kings Medical College withou proval from the Kenya Medica oratory Technicians and Tech gists Board. The former governme pathologist was charged alongside the co-director of the college L Kanyiri and two lecturers — L Muriithi and Evans Orwaru. T medical college is in Kieni Eas Sub-County, Nyeri. The case wi heard on March 16.

—*Joseph Wang*

KIRINYAGA

Man in wife murder case to be detained for 10 d

A man accused of killing his will remain in custody for 10 da allow police complete their inve gations. The court was told tha the Nazario Muriuki Mbogo beheaded his wife on Saturday. He was pr sented in court yesterday but di not take plea. According to the ecution, Mr Mbogo killed his w and locked the body in the house. The two had earlier in the day attended a parents' meeting at th son's school. Moments after ret ing home, the woman was hear screaming. Neighbours arrived utes later and found the body.

—*Nicholas Kom*

Philanthropy | Her love for children birthed life-long journey

Kibera woman feeds 37 children all on her own

One night in June 2002, strangers knocked on her door and dropped off two boys found on the streets. This marked the beginning of her journey.

By Gardy Chacha
gchacha@standardmedia.co.ke

To get to Pamela Owino's house, one must navigate a labyrinth of narrow alleys. In Kibera, where she lives, most residents' top priority is putting food on the table.

"With food in your stomach you can survive another day," says Ms Owino.

Fifteen years ago, Owino, 54, was your average woman surviving on small business ventures. But she was also known for her friendliness towards children.

"I used to interact with girls who had had babies and were struggling with providing for them and motherhood issues," she recalls.

"I would watch their children as they went to buy small items for sale. They used the profits to feed their children."

Pamela's children

- The youngest of the 37 children is two while the oldest is 15 years
- She spends approximately Sh1,800 daily to put food on the table
- She farms sugarcane on a leased plot of land in Chemelil and use the earnings for food

Past midnight

One night – well past midnight – in June 2002, strangers knocked on her door and dropped off two boys.

"They said they picked the boys from the streets hungry and with nowhere to sleep. Someone led them to my house – because apparently I was helping small children," she says.

The boys, it turned out, had been chased from home by their mother. The woman had become suicidal after being dumped by her husband who (she had just discovered) had infected her with HIV.

"My husband and I were shocked," Owino says. "Not to mention that we had five children of our own that we needed to look after."

But the strangers hadn't come to debate whether they should leave the boys with her or take them away.

"I just couldn't refuse to accommodate them, at least for the night."

The next day, Owino confronted the boys' mother, who swore she would kill them if Owino forced her to take them back. And just like that, she became a mother of two more children. Her gesture attracted more people to drop off children and by 2006, she had 31.

"Somehow my husband and I made just enough to buy us food," she says.

Donated food

Once in a while, well-wishers donated food and money. Between 2008 and 2011, Owino worked at the United Nations Development Programme on contract. It was her salary that kept the family going.

But at some point, her husband left, saying she had to choose between him and the children.

"I couldn't chase the children away; they were totally innocent. So my husband left for another woman," she says.

Over the years, 145 children have gone through Owino's home. Today she still has 37 who are in school and who depend on her for food and fees.

Pamela Owino, 54, who cares for children using her own resources. The children are mostly dumped by their parents or are orphans from diverse backgrounds. [Gardy Chacha, Standard]

REPUBLIC OF KENYA

NATIONAL ASSEMBLY
TWELFTH PARLIAMENT – FIRST SESSION
In the Matter of consideration by the National Assembly - The Copyright (Amendment) Bill, 2017

SUBMISSION OF MEMORANDA

Article 118(1)(b) of the Constitution provides that, *"Parliament shall facilitate public participation and involvement in the legislative and other business of Parliament and its Committees".*

Further, Standing Order 127(3) provides that, *"the Departmental Committee to which a Bill is committed shall facilitate public participation and shall take into account views and recommendations of the public when the Committee makes its report to the House".*

The Copyright (Amendment) Bill, 2017 seeks to amend several clauses of the Copyright Act 2001.The general objective of the amendments is to expand the scope of copyright protection, add extensive protection in respect of broadcasts and signals, promote sound corporate governance and improve efficiency in royalty collection.
The Copyright (Amendment) Bill, 2017, has undergone First Reading pursuant to Standing Order 127(3) and is now committed to the **Departmental Committee on Communications, Information and Innovation** for consideration and thereafter report to the House.

Pursuant to Article 118(1) (b) and Standing Order 127(3), the Committee invites members of the Public to submit any representations they may have on the **Copyright** (Amendment) Bill, 2017. The representations may be forwarded to the **Clerk of the National Assembly, P.O. Box 41842-00100, Nairobi;** hand-delivered to the **Office of the Clerk, Main Parliament Buildings, Nairobi;** or emailed to **clerk@parliament.go.ke;** to be received on or before **Tuesday 13th February, 2018 at 5:00 pm.**

MR. MICHAEL R. SIALAI, EBS
CLERK OF THE NATIONAL ASSEMBLY

REPUBLIC OF KENYA

NATIONAL ASSEMBLY
TWELFTH PARLIAMENT – FIRST SESSION
In the Matter of consideration by the National Assembly - The Computer and Cybercrimes Bill, 2017

SUBMISSION OF MEMORANDA

Article 118(1) (b) of the Constitution provides that, *"Parliament shall facilitate public participation and involvement in the legislative and other business of Parliament and its Committees".*

Further, Standing Order 127(3) provides that, *"the Departmental Committee to which a Bill is committed shall facilitate public participation and shall take into account views and recommendations of the public when the Committee makes its report to the House".*

The Computer and Cybercrimes Bill, 2017 proposes to provide a framework to prevent and control the threat of cybercrime, that is, offences against computer systems and offences committed by means of computer systems.
The Computer and Cybercrimes Bill, 2017, has undergone First Reading pursuant to Standing Order 127(3) and is now committed to the **Departmental Committee on Communications, Information and Innovation** for consideration and thereafter report to the House.

Pursuant to Article 118(1)(b) and Standing Order 127(3), the Committee invites members of the Public to submit any representations they may have on the Computer and Cybercrimes Bill, 2017. The representations may be forwarded to the **Clerk of the National Assembly, P.O. Box 41842-00100, Nairobi;** hand-delivered to the **Office of the Clerk, Main Parliament Buildings, Nairobi;** or emailed to **clerk@parliament.go.ke;** to be received on or before **Tuesday 13th February, 2018 at 5:00 pm.**

MR. MICHAEL R. SIALAI, EBS
CLERK OF THE NATIONAL ASSEMBLY

MINUTES OF THE 21ST SITTING OF THE COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN 5TH FLOOR, CONTINENTAL HOUSE ON MONDAY 19TH MARCH 2018, AT 2.00 P.M.

PRESENT

1. Hon. William Kipkemoi, M.P. **-Chairperson**
2. Hon. George Macharia kariuki, M.P. **-Vice- Chairperson**
3. Hon. Maritim Sylvanus, M.P.
4. Hon. Jonah Mburu, M.P.
5. Hon. Alfah O. Miruka, M.P.
6. Hon. Marwa Kitayama Maisori, M.P.
7. Hon. Mwambu Mabongah, M.P.
8. Hon. Erastus Nzioka Kivasu, M.P.
9. Hon. Innocent Momanyi Obiri, M.P
10. Hon. Gertrude Mbeyu Mwanyanje, M.P.
11. Hon. Wamuchomba Gathoni, M.P.
12. Hon. Annie Wanjiku Kibeh,M.P

APOLOGIES

1. Hon. Joshua Kimilu Kivinda, M.P.
2. Hon. Anthony Tom Oluoch, M.P.
3. Hon. (Eng.). Mark Nyamita, M.P
4. Hon. Godfrey Osotsi Atieno, M.P
5. Hon. John Kiarie Waweru, M.P
6. Hon. Liza Chelule Chepkorir ,M.P
7. Hon. Mwangaza Kawira, M.P

National Assembly Secretariat

1.	Ms Ella Kendi	Clerk Assistant III
2.	Mr. Sidney Lugaga	Legal Counsel II
3.	Ms.Catherine Gati	Fiscal Analst
4.	Mr.Elijah Ichwara	Audio officer

MINUTE NO.076/2018: PRELIMINARIES

The Chairperson called the meeting to order at twenty minutes past two o'clock followed with a word of prayer

MINUTE NO.077/ 2018: ADOPTION OF THE REPORT ON CONSIDERATION OF THE COMPUTER AND CYBERCRIMES BILL, 2017

The Committee considered the report on consideration of the Computer and Cybercrimes Bill, 2017 and adopted it with the following recommendations;

CLAUSE 2

THAT, Clause 2 of the Bill be amended—

(a) by deleting the definition of "authorised person" and substituting therefor the following new definition—

"authorised person" means an officer in a law enforcement agency or a cybersecurity expert designated by the Cabinet Secretary responsible for matters relating to national security by notice in the *Gazette* for the purposes of Part III of this Act."

(b) by deleting the definition of "Authority" and substituting therefor the following new definition—

""Authority" means the Communications Authority of Kenya";

(c) by deleting the definition of "Central Authority" and substituting therefor the following new definition—

""Central Authority" means the Office of the Attorney General";

(d) in the definition of "premises" by inserting the words "a physical or virtual space in which data is maintained, managed, backed up remotely and made available to users over a network" immediately after the word "aircraft";

(e) by deleting the definition of "requested state" and substituting therefor the following new definition—

""requested state" means a state being requested to provide legal assistance under the terms of this Act";

(f) by deleting the definition of "requesting state" and substituting therefor the following new definition—

""requesting state" means a state requesting for legal assistance and may for the purposes of this Act include an international entity to which Kenya is obligated";

(g) by inserting the following new definitions in the proper alphabetical sequence—

"national critical information infrastructure" means a vital virtual system and asset whose incapacity, destruction or modification would have a debilitating impact on the security, economy, public health or safety of the country;

Justification: For the purpose of clarity.

CLAUSE 3

THAT, clause 3 of the Bill be amended—

(a) by deleting paragraph (c) and substituting therefor the following new paragraph—

"(c) facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes";

(b) in paragraph (c) by inserting the following new paragraph immediately after paragraph (c)—

"(ca) protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution;"

Justification: To include the facilitation, prevention, detection and punishment of cybercrime and the protection of the human rights in cyberspace as part of the objects of the Bill.

CLAUSE 5

THAT, clause 5 of the Bill be amended in subclause (2) by deleting the word "this" appearing immediately after the words "purposes of";

Justification: To ensure consistency and clarity of the Clause

CLAUSE 7

THAT, clause 7 of the Bill be amended in subclause (2) by deleting the word "of" appearing immediately after the words "for a term" at the end of the subclause;

Justification: To rectify typographical errors

CLAUSE 8

THAT, clause 8 of the Bill be amended—

(a) in subclause (2) by deleting the words "without sufficient excuse or justification" appearing immediately after the words "this Part";

(b) in subclause (3) by deleting the words "in thereof" appearing immediately after the word "described" and substituting therefor the words "under the subsections";

Justification: The phrase "without sufficient excuse or justification" contradicts the intent of subclause (2). No sufficient excuse or justification exists for knowingly receiving or being possession of a program, password, device, access code or similar data and intending that it be used to commit or assist in the commission of an offence.

CLAUSE 9

THAT, clause 9 of the Bill be amended in subclause (1) by deleting the word "term" appearing immediately after the word "imprisonment";

Justification

To rectify a typographical error.

CLAUSE 10

THAT, clause 10 of the Bill be amended—

(a) in subclause (1) by inserting the words "for a" immediately after the word "imprisonment"

(b) in subclause (2)(f) by deleting the words "by the Cabinet Secretary in the manner or form as the Cabinet Secretary may consider appropriate" and substituting therefor the words—

> "relating to the security, defence or international relations of Kenya, critical information, communications, business or transport infrastructure and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication and technology."

Justification:

(i) To correct a typographical error; and

(ii) To prescribe the purposes for which the Cabinet Secretary may designate a system to be a protected system under the Bill.

CLAUSE 11

THAT, clause 11 of the Bill be amended in subclause (3) by inserting the word "shillings" immediately after the words "five million";

Justification: To rectify a typographical error.

CLAUSE 12

THAT, clause 12 of the Bill be amended by—

(a) renumbering the existing provision as subclause (1);

(b) inserting the following new subclause immediately after subclause (1)—

"(2) Pursuant to Article 24 of the Constitution, the freedom of expression under Article 33 of the Constitution shall be limited in respect of the intentional publication of false, misleading or fictitious data or misinformation that—

(a) is likely to—

(i) propagate war; or

(ii) incite persons to violence;

(b) constitutes hate speech;

(c) advocates hatred that—

(i) constitutes ethnic incitement, vilification of others or incitement to cause harm; or

(ii) is based on any ground of discrimination specified or contemplated in Article 27(4) of the Constitution; or

(d) negatively affects the rights or reputations of others.

Justification: To provide the extent of limitation of the freedom of expression as required by Article 24(2) of the Constitution..

CLAUSE 13

THAT, clause 13 of the Bill be deleted;

Justification: To transfer the proposals under the clause to a harmonized amendment to the Sexual Offences Act, 2011.

CLAUSE 16

THAT, clause 16 of the Bill be amended—

(a) by deleting the marginal note and substituting therefor the following marginal note—

"cyber harassment";

(b) in subclause (1) by deleting the words "and repeatedly" appearing in the opening statement;

(c) by inserting the following new subclauses immediately after subclause (3)—

"(4) A person may apply to Court for an order compelling a person charged with an offence under subclause (1) to refrain from—

(a) engaging or attempting to engage in; or

(b) enlisting the help of another person to engage in,

any communication complained of under subsection (1);

(5) The Court—

(a) may grant an interim order; and

(b) shall hear and determine an application under subsection (4) within fourteen days.

(6) An intermediary may apply for the order under subsection (4) on behalf of a complainant under this section.

(7) A person may apply for an order under his section outside court working hours.

(8) The Court may order a service provider to provide any subscriber information in its possession for the purpose of identifying a person whose conduct is complained of under this section.

(9) A person who contravenes an order made under this section commits an offence and is liable, on conviction to a fine not exceeding one million shillings or to imprisonment for a term not exceeding six months, or to both.

Justification: Cyber harassment covers the two aspects of cyber bullying and cyber stalking. The amendment also allows for a victim to apply for a restraining order.

NEW CLAUSES

THAT, the Bill be amended by inserting the following new clauses immediately after clause 16—

Cybersquatting	**16A.** A person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network, without authority or right, commits an offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.
Wrongful distribution of intimate images.	**16B.** A person who transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate image of another person commits an offence and is liable, on conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding thirty years or to both.
Identity theft and impersonation.	**16C.** A person who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person commits an offence and is liable, on conviction, to a fine not exceeding two hundred thousand shillings or to imprisonment for a term not exceeding three years or both.
Phishing.	**16D.** A person who creates or operates a website or sends a message through a computer system with the intention to induce the user of a website or the recipient of the message to disclose personal information for an unlawful purpose or to gain unauthorized access to a computer system, commits an offence and is liable upon conviction to a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding three years or both.
Interception of electronic messages or money transfers.	**16E.** A person who unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed commits an

offence and is liable on conviction to a fine not exceeding two hundred thousand shillings or to a term of imprisonment not exceeding seven years or to both.

Willful misdirection of electronic messages.

16F. A person who willfully misdirects electronic messages commits an offence and is liable on conviction to a fine not exceeding one hundred thousand shillings or to imprisonment for a term not exceeding two years or to both.

Justification:

To include the offences of Cyber squatting, Wrongful distribution of intimate images, phishing, Interception of electronic messages or money transfers, and Willful misdirection of electronic messages as offences under the Bill.

CLAUSE 21

THAT, the Bill be amended by deleting clause 21 and substituting therefor the following new Clause—

Additional penalty for other offences committed through use of a computer system.

21. (1) A person who commits an offence under any other law through the use of a computer system commits an offence and shall be liable on conviction to a penalty similar to the penalty provided under that law.

(2) A Court shall, in determining whether to sentence a person convicted of an offence under this section, consider—

(a) the manner in which the use of a computer system enhanced the impact of the offence;

(b) whether the offence resulted in a commercial advantage or financial gain;

(c) the value involved, whether of the consequential loss or damage caused, or the profit gained from commission of the offence through the use of a computer system;

(d) whether there was a breach of trust or responsibility;

(e) the number of victims or persons affected by the offence;

(f) the conduct of the accused; and

(g) any other matter that the court deems fit to consider.

Justification: To make the use of computer technology to commit offences covered under other laws as constituting an aggravated offence with a penalty similar to the penalty set out in the law governing the initial offence. Under the revised clause, the Court will have a discretion to consider the circumstances of each case before applying the enhanced sentence.

CLAUSE 23

THAT, clause 23 of the Bill be amended—

(a) in subclause (7) by inserting the following new paragraphs immediately after paragraph (b)—

"(c) maintain the integrity of a computer system, any data or information accessed or retained; and

(d) maintain the confidentiality of a computer system, any data or information accessed during the execution of the warrant."

(b) in sub clause (8) by deleting paragraph (b) and substituting therefor the following new paragraph—

"(b) compromises the integrity or confidentiality of a computer system, data or information accessed or retained under this section or misuses the powers granted under this section,

commits an offence and is liable on conviction to a fine not exceeding five million shillings or to a term of imprisonment not exceeding three years or to both."

Justification: To require investigating authorities to maintain integrity and confidentiality of information seized while executing a search warrant.

CLAUSE 24

THAT, Clause 24 be deleted

Justification: There exists no justification to conduct a search without a warrant. The provision, additionally, contradicts Article 24(2) and 31 of the Constitution.

CLAUSE 26

THAT, clause 26 of the Bill be amended by—

(a) deleting subclause (4);

Justification: The requirement to maintain confidentiality of the existence of an order under the clause is not necessary.

(b) deleting subclause (6);

Justification: The clause violates the right to privacy. The police or the authorized persons under the Act should seek permission from the Court before compelling the production of data or subscriber information.

CLAUSE 27

THAT, clause 27 of the Bill be amended—

(a) in subclause (2) by deleting the words "the period specified in the notice" and substituting therefor the words "thirty days"

Justification: To define time limit for preservation of traffic data.

(b) by deleting subclause (4);

Justification: The requirement to maintain confidentiality of the existence of an order under the clause is not necessary.

CLAUSE 28

THAT, clause 28 of the Bill be amended

(a) in subclause (4) by deleting the word "not" appearing immediately after the words "for a period";

(b) in subclause (7) by inserting the word "shillings" immediately after the words "ten million" appearing in paragraph (a);

Justification: To rectify typographical errors

CLAUSE 29

THAT, clause 29 of the Bill be amended—

(a) in subclause (1) by deleting the words "a serious" appearing immediately after the words "in respect of" in the opening statement and substituting therefor the words "an";

(b) in subclause (7)(a) by inserting the word "shillings" immediately after the words "ten million";

Justification: To delete a subjective reference and to rectify a typographical error.

CLAUSE 33

THAT, clause 33 of the Bill be amended—

(a) in subclause (1) by inserting the words " the Extradition (Contiguous and Foreign Countries) Act" immediately after the phrase "2011".

(b) in subclause (4) by inserting the words " the Extradition (Contiguous and Foreign Countries) Act" immediately after the phrase "2011".

Justification: To include a reference to the Etradition (Contigous and Foreign Countries Act). The two Acts are complimentary in ensuring successful prosecution of offences under the Bill.

CLAUSE 38

THAT, clause 38 of the Bill be amended by deleting—

(a) the word "another" wherever it appears;

Justification: to rectify a typographical error.

(b) the words "without the authorisation but" appearing immediately after the word "may" in the opening statement;

Justification: the phrase contradict the intent of the clause.

(c) the phrase "(open source)" appearing in paragraph (a);

Justification: to enhance the clarity of the clause.

CLAUSE 39

THAT, clause 39 of the Bill be amended in subclause (2)(g) by inserting the words "to the" immediately after the word "relevant";

Justification: to correct a typographical error.

CLAUSE 41

THAT, clause 41 of the Bill be amended in subclause (1) by deleting the words "and prosecuting" appearing immediately after the word "investigating".

Justification: The Central Authority established under ether Bill falls under the purview of the Office of the Attorney General who does not have the prosecutorial powers under the Constitution.

CLAUSE 46

THAT, the Bill be amended by deleting Clause 46 and substituting therefor the following new clause—

PART VI—PROVISIONS ON DELEGATED POWERS

Regulations.

46. (1) The Cabinet Secretary may make regulations generally for the better carrying into effect of any provisions under this Act.

(2) Without prejudice to the foregoing, regulations made under this section may provide for standard operating procedures for the conduct, search, seizure and collection of electronic evidence.

(3) For the purposes of Article 94 (6) of the Constitution—

(a) the purpose and objective of delegation under this section is to enable the Cabinet Secretary to make regulations to provide for the better carrying into effect of the provisions of this Act and to enable the Authority to discharge its functions more effectively;

(b) the authority of the Cabinet Secretary to make regulations under this Act will be limited to bringing into effect the provisions of this Act and to fulfil the objectives specified under this section;

(c) the principles and standards applicable to the regulations made under this section are those set out in the Interpretation and General Provisions Act and the Statutory Instruments Act, 2013.

Cap 2,
No. 23 of 2013

Justification: To comply with the provisions of Article 94(6) of the Constitution;

SCHEDULE

THAT, the Schedule to the Bill be amended by inserting the following amendments to the Sexual Offences Act—

The Sexual offences Act be amended by—

(a) deleting Section 16 and substituting therefor the following new section—

16. Child pornography

(1) A person, including a juristic person, who knowingly—

(a) possesses an indecent photograph of a child;

(b) displays, shows, exposes or exhibits obscene images, words or sounds by means of print, audio-visual or any other media to a child with intention of encouraging or enabling a child to engage in a sexual act;

(c) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or has in his or her possession an indecent photograph of a child;

(d) imports, exports or conveys any obscene object for any of the purposes specified in subsection (1), or knowingly or having reason to believe that such object will be sold, let to hire, distributed or publicly exhibited or in any manner put into circulation;

(e) takes part in or receives profits from any business in the course of which he or she knows or has reason to believe that obscene objects are, for any of the purposes specifically in this section, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation;

(f) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be produced from or through any person; or

(g) offers or attempts to do any act which is an offence under this section,

commits an offence and is liable upon conviction to imprisonment for a term of not less than six years or to a fine of not less than five hundred thousand shillings or to both and upon subsequent conviction, to imprisonment to a term of not less than seven years without the option of a fine.

(2) This section shall not apply to—

(a) Publication or possession of an indecent photograph where it is proved that such publication or possession was intended for bona fide scientific research, medical, religious or law enforcement purpose; the indecent representation of a child in a sculpture, engraving, painting or other medium on or in any ancient monument recognised by law; and

(b) activities between two persons above eighteen years of age by mutual consent.

(3) For the purposes of subsection (1),—

(a) an image is obscene if—

(i) it is lascivious or appeals to prurient interest; or

(ii) its effect, or where it comprises two or more distinct items, the effect of any one of its items, if taken as a whole, tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

(b) an indecent photograph includes a visual, audio or audio visual representation depicting—

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; or realistic images representing a child engaged in sexual activity.

(b) inserting the following new section immediately after section 16—

Sexual communication with a child

16A. (1) A person of eighteen years and above who knowingly communicates with a child in—

(i) a sexual manner; or

(ii) a manner intended to encourage the child to communicate in a sexual manner,

commits an offence and is liable, on conviction, to a fine of not less than five hundred thousand shillings or imprisonment for a term of not less than five years, or to both.

(2) For the purposes of this section, a communication is sexual if—

(a) any part of it relates to sexual activity, or

(b) a reasonable person would consider any part of the communication to be sexual.

Justification:

(i) To amend section 16 of the Sexual Offences Act, 2011 to harmonize its provisions with the provisions of the deleted clause 13; and

(ii) To provide for the offence of sexual communication with a child (grooming) in the Sexual Offences Act, 2011.

~~MINUTE NO.078/2018:~~ ~~ADJOURNMENT~~

There being no other business, the sitting adjourned at 4.30pm. The next meeting to be held on Tuesday 20th March, 2018 at 8.30am.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 19TH SITTING OF THE COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN 9TH FLOOR HARAMBEE, PLAZA ON TUESDAY 13TH MARCH 2018, AT 11.00 A.M.

PRESENT

1. Hon. George Macharia kariuki, M.P. **-Vice- Chairperson**
2. Hon. Maritim Sylvanus, M.P.
3. Hon. Joshua Kimilu Kivinda, M.P.
4. Hon. John Kiarie Waweru, M.P
5. Hon. Alfah O. Miruka, M.P.
6. Hon. Marwa Kitayama Maisori, M.P.
7. Hon. Mwangu Mabongah, M.P.
8. Hon. Erastus Nzioka Kivasu, M.P.
9. Hon. Anthony Tom Oluoch, M.P.
10. Hon. Gertrude Mbeyu Mwananje, M.P.
11. Hon. Wamuchomba Gathoni, M.P.
12. Hon. Annie Wanjiku Kibeh,M.P
13. Hon. (Eng.). Mark Nyamita, M.P
14. Hon. Godfrey Osotsi Atieno, M.P

APOLOGIES

1. Hon. William Kipkemoi, M.P. **-Chairperson**
2. Hon. Jonah Mburu, M.P.
3. Hon. Liza Chelule Chepkorir ,M.P
4. Hon. Mwangaza Kawira, M.P
5. Hon. Innocent Momanyi Obiri, M.P

IN ATTENDANCE

National Assembly Secretariat

1.	Ms Ella Kendi	Clerk Assistant III
2.	Mr. Ronald Walala	Legal Counsel II
3.	Ms.Lorna Okatch	Research Officer III
4.	Ms.Fatuma Abdi	Audio officer
5.	Mr. Wilson Angatangoria	Sergeant- at- arms

MINUTE NO.067/2018: PRELIMINARIES

The Chairperson called the meeting to order at twenty minutes past eleven o'clock followed with a word of prayer

MINUTE NO.068/ 2018: CONFIRMATION OF MINUTES

The confirmation of the minutes of the previous sitting was deferred to the next meeting.

MINUTE NO.069/2018: CONSIDERATION OF THE DRAFT REPORT ON COMPUTER AND CYBERCRIMES BILL, 2017

The Committee Members were taken through the recommendations Clause by Clause as follows;

1. Clause 2: Agreed to

It was indicated that there was need to elaborate the definition of the term 'national critical information infrastructure' by including the aspect of interference or modification of the virtual system.

2. Clause 3: Agreed to
3. Clause 11: Agreed to
4. Clause 12: Agreed to
5. Clause 13: Agreed to
6. Clause 16: 'Delete the word 'repeatedly' to ensure that an offence committed once is charged.
7. Clause 16(9) the Committee proposed the fine as one Million Kenya Shillings or an imprisonment of a term not exceeding six months.
8. Clause 21: Agreed to
9. Clause 23: Agreed to

MINUTE NO.070/2018: ADJOURNMENT

There being no other business, the sitting adjourned at 1.30pm.

Signed.....

(Chairperson)

Date.....1/9/03/2018.....

MINUTES OF THE 18TH SITTING OF THE COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD AT WESTON HOTEL, NAIROBI ON SATURDAY 10TH MARCH 2018, AT 2.30 P.M.

PRESENT

1. Hon. Kisang' William Kipkemoi, M.P. - **Chairman**
2. Hon. George Macharia kariuki, M.P. - **Vice- Chairperson**
3. Hon. Maritim Sylvanus, M.P.
4. Hon. Joshua Kimilu Kivinda, M.P.
5. Hon. Jonah Mburu, M.P.
6. Hon. Godfrey Osotsi Atieno, M.P
7. Hon. John Kiarie Waweru, M.P
8. Hon. Wamuchomba Gathoni, M.P.
9. Hon. Annie Wanjiku Kibeh,M.P

APOLOGIES

1. Hon. Alfah O. Miruka, M.P.
2. Hon. Marwa Kitayama Maisori, M.P.
3. Hon. Mwangu Mabongah, M.P.
4. Hon. Erastus Nzioka Kivasu, M.P.
5. Hon. Liza Chelule Chepkorir ,M.P
6. Hon. Mwangaza Kawira, M.P
7. Hon. Anthony Tom Oluoch, M.P.
8. Hon. Gertrude Mbeyu Mwananje, M.P.
9. Hon. (Eng.). Mark Nyamita, M.P
10. Hon. Innocent Momanyi Obiri, M.P

IN ATTENDANCE

National Assembly Secretariat

1. Mr. Nicholas Emejen - Deputy Director, Committee Services
2. Mr. Ronald Walala - Legal Counsel II
3. Ms Ella Kendi - Clerk Assistant III
4. Ms. Catherine Gati - Fiscal Analyst III
5. Ms. Betty Auma - Secretary
6. Mr. Rahab Chepkilim - Audio officer
7. Mr. Wilson Angatangoria - Sergeant- at- arms

MINUTE NO.062/2018: PRELIMINARIES

The Chairperson called the meeting to order at 2.45p.m and thereafter welcomed all the members present.

MINUTE NO.063/ 2018: CONFIRMATION OF MINUTES

The confirmation of the minutes of the previous sitting was deferred to the next meeting.

MINUTE NO.064/2018: CONSIDERATION OF THE MEMORANDA ON THE COMPUTER AND CYBERCRIMES BILL, 2017.

Clause 35

The Committee agreed with provisions of clause 35 and that there was no memoranda received relating to the Clause

Clause 36

The Committee agreed with provisions of clause 36 and that there was no memoranda received relating to the Clause.

Clause 37

The Committee agreed with provisions of clause 37 and that there was no memoranda received relating to the Clause.

Clause 38

Article 19 sought deletion of the Clause while Michael Odhiambo proposed for an amendment. The Committee agreed with the two proposals to the extent that the Clause contains inherent contradiction with the inclusion of the phrase 'without authorisation'. The Committee therefore noted there was need to delete the phrase to cure the contradiction.

Clause 39

The Committee agreed with provisions of clause 39 and that there was no memoranda received relating to the Clause.

Clause 40

The Committee agreed with provisions of clause 40 and that there was no memoranda received relating to the Clause.

Clause 41

CAK and Ministry of ICT: The Committee agreed with the proposal noting that the Central Authority established under the Bill falls under the purview of the Office of the Attorney General who does not have prosecutorial powers under the Constitution.

Clause 42,43,44 and 45

The Committee agreed with provisions of clauses 42,43, 44 and 45 and that there was no memoranda received relating to the Clause.

Clause 46

The Committee had not received any memoranda relating to the Clause. In its deliberation it was noted that there was need to amend the Clause in compliance with the provisions of the Constitution which requires an Act of Parliament that delegates legislative powers to expressly specify the purpose and objectives for which that authority is conferred.

Additional proposals

Hon.Godfrey Otsosi, MP presented the Committee the following proposals and comments on the Bill as follows;

1. There was need to provide a clear definition of the term National Critical Information Infrastructure in the Bill. The Committee to take into consideration the following aspects when defining the;
    I. Designation of the Computer System eg inclusion of IFMIS, KRA IEBC and bank systems
    II. There should be a structured process of Auditing and Inspecting the system
    III. Ways of handling the offence committed
    IV. Take into consideration the best practices.
2. There was need to align the Bill with Antiterrorism Act to incorporate the cyber terrorism aspect in the Bill.
3. Proposed to change the title of the Bill to 'Computer Misuse and Cybercrimes' as the current title was general.
4. Based on analysis of other jurisdiction there was need to establish a body that will ensure the administration and enforcement of the Bill.
5. Proposed inclusion of the following under the objects the Act;
   Clause 3 (c) add the words 'prevention, detection and punishment'

MINUTE NO.065//2018: ANY OTHER BUSINESS

The members were reminded that there was need to expedite the Bill so as have it tabled on the floor of the House in the week of 19th March 2018.

MINUTE NO.066/2018: ADJOURNMENT

There being no other business, the sitting adjourned at 5.00 pm. Next sitting of the committee was to be held on Tuesday, 13th March 12, 2018 at 11.00 a.m.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 17TH SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD AT WESTON HOTEL, NAIROBI ON 10TH MARCH 2018, AT 11.00 A.M.

PRESENT

1. Hon. William Kipkemoi, M.P. - **Chairperson**
2. Hon. George Macharia kariuki, M.P. - **Vice- Chairperson**
3. Hon. Maritim Sylvanus, M.P.
4. Hon. Joshua Kimilu Kivinda, M.P.
5. Hon. Jonah Mburu, M.P.
6. Hon. Godfrey Osotsi Atieno, M.P
7. Hon. John Kiarie Waweru, M.P
8. Hon. Annie Wanjiku Kibeh,M.P
9. Hon. Wamuchomba Gathoni, M.P.

APOLOGIES

1. ~~Hon. Alfah O. Miruka, M.P.~~
2. Hon. Marwa Kitayama Maisori, M.P.
3. Hon. Mwangu Mabongah, M.P.
4. Hon. Erastus Nzioka Kivasu, M.P.
5. Hon. Liza Chelule Chepkorir ,M.P
6. Hon. Mwangaza Kawira, M.P
7. Hon. Anthony Tom Oluoch, M.P.
8. Hon. Gertrude Mbeyu Mwananje, M.P.
9. Hon. (Eng.). Mark Nyamita, M.P
10. Hon. Innocent Momanyi Obiri, M.P

IN ATTENDANCE

National Assembly Secretariat

1. Mr. Nicholas Emejen - Deputy Director, Committee Services
2. Mr. Ronald Walala - Legal Counsel II
3. ~~Ms Ella Kendi~~ - Clerk Assistant III
4. Ms. Catherine Gati - Fiscal Analyst III
5. Ms. Betty Auma - Secretary
6. Mr. Rahab Chepkilim - Audio officer
7. Mr. Wilson Angatangoria - Sergeant- at- arms

MINUTE NO.058/2018: PRELIMINARIES

The Chairperson called the meeting to order at 11.00 am followed with a word of prayer.

MINUTE NO.059/ 2018: CONFIRMATION OF THE MINUTES

The confirmation of the minutes of the previous sitting was deferred to the next meeting. Therefore there were no matters arising.

MINUTE NO.060/2018: CONSIDERATION OF THE MEMORANDA ON THE COMPUTER AND CYBERCRIMES BILL, 2017.

Clause 27 (2):

(i) The Committee agreed with the submission by ISACA-KENYA and Safaricom to delete the words 'the period specified in the notice' and substitute it with the words 'thirty days'. The committee agreed that there was need to provide a definite period in the preservation of the traffic data.

(ii) The Committee agreed with the submission by Safaricom to delete sub clause 4 as it contravenes section 15 of KICA Consumer protection regulations 2010 which require that a service provider maintain the confidentiality of a service provider maintain the confidentiality of a customer's information and communications.

Clause 28

(i) The Committee resolved to amend sub clause 4 by deleting the word 'not'

(ii) The Committee disagreed with the submission of ISACA KENYA and KICTANET to reduce the period of collecting real time data from noting that the time is reasonable as the complexity of the investigations conducted under the Bill may vary.

(iii)Safaricom Ltd; the Committee disagreed with their proposal citing that its inclusion as a requirement under the Clause would hamper execution of a validly obtained Court Order in the event the proposed Principal Officer of person acting in a similar capacity in unavailable is or uncooperative.

(iv)CIPIT: The Committee agreed with their submission and noted the need to amend the Bill to limit the persons authorised to apply for Court Orders or search warrants to persons above the rank of Chief Inspector of Police in order to prevent abuse of the powers granted under the Bill by investigative agencies.

(v) The committee disagreed with the submission by TESPOK to define 'stored data' as the words have a common meaning.

(vi)The committee disagreed with the submission by KEPSA to replace the word 'may' by 'shall' as the use of the word 'may' gives someone the discretion to or not obtain a court order.

Clause 29

1. Article 19, TESPOK and KICTANET: The Committee disagreed with their proposal noting that the Clause is an inclusion in the Bill which allows the police or authorized persons to access the content data of communications to assist them in monitoring and prevention of cybercrime.
2. The Committee disagreed with the views of Safaricom Ltd citing that sub clause (1) provides an adequate safeguard against arbitrary violation of the right to privacy by requiring investigation agencies to first obtain a court order for which they must give reasons.
3. KEPSA: The Committee disagreed noting that the term may as used in the Clause adequately makes it mandatory for the police or authorised persons to obtain an order from the Court before seeking the real time collection or recording of content data for the purposes of investigations.

Clause 30

The committee was informed that there was no memorandum submitted in relation to clause 30

Clause 31

The committee was informed that there was no memorandum submitted in relation to Clause 30

Clause 32

The committee disagreed with the submission by KEPSA noting that the Clause as drafted adequately covers the issue of protecting service providers from incurring any liability as a result of complying with orders issued by the Court under the provisions of the Bill.

Clause 33

The committee agreed with the provisions of Clause 33 and that there was no memorandum submitted in relation to the Clause 33.

Clause 34

The committee disagreed with the submission by the centre for intellectual property and information technology law to have judicial oversight in the clause as this would result to compromised independence.

MINUTE NO.061/ /2018: ADJOURNMENT

There being no other business, the sitting adjourned at 1.30 pm. Next sitting of the committee was to be held on the same day at 2.30 p.m. at Weston Hotel, Nairobi.

Signed.....(Chairperson

Date.....19/03/2018.....

MINUTES OF THE 16TH SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN WESTON HOTEL, NAIROBI ON FRIDAY 9TH MARCH 2018, AT 2.00 P.M.

PRESENT

1. Hon. Kisang' William Kipkemoi, M.P. - **Chairperson**
2. Hon. George Macharia kariuki, M.P. - **Vice- Chairperson**
3. Hon. Annie Wanjiku Kibeh,M.P
4. Hon. Joshua Kimilu Kivinda, M.P.
5. Hon. Maritim Sylvanus, M.P.
6. Hon. Jonah Mburu, M.P.
7. Hon. Wamuchomba Gathoni, M.P.
8. Hon. John Kiarie Waweru, M.P
9. Hon. Godfrey Osotsi Atieno, M.P

APOLOGIES

1. Hon. Liza Chelule Chepkorir ,M.P
2. Hon. Marwa Kitayama Maisori, M.P.
3. Hon. Mwambu Mabongah, M.P.
4. Hon. Erastus Nzioka Kivasu, M.P.
5. Hon. Alfah O. Miruka, M.P.
6. Hon. Mwangaza Kawira, M.P
7. Hon. Anthony Tom Oluoch, M.P.
8. Hon. Gertrude Mbeyu Mwanyanje, M.P.
9. Hon. (Eng.). Mark Nyamita, M.P
10. Hon. Innocent Momanyi Obiri, M.P

IN ATTENDANCE

National Assembly Secretariat

1. Mr. Nicholas Emejen - Deputy Director, Committee Services
2. Ms.Ella Kendi - Clerk Assistant III
3. Ms. Catherine Gati - Fiscal Analyst
4. Mr. Ronald Walala - Legal Counsel
5. Ms.Beatrice Auma - Secretary
6. Ms.Rahab Chepkilim - Audio officer
7. Mr. Wilson Angatangoria - Sergeant- at- arms

MINUTE NO. 054/2018: PRELIMINARIES

The Chairperson called the meeting to order at twenty minutes past two o'clock followed with a word of prayer.

MINUTE NO.055/ 2018: CONFIRMATION OF MINUTES

The confirmation of the minutes of the previous sitting was deferred to the next meeting.

MINUTE NO.056/2018: CONSIDERATION OF THE SUBMISSION FOR THE COMPUTERS AND CYBERCRIME BILL, 2017

The Legal Counsel took the Members though the memoranda as follows;

Clause 21

1. Article 19 proposal was disagreed with citing that the Clause is necessary in the Bill to cater for instances where ordinary offences are committed through the use of Computer forgery.
2. KICTANET proposal was agreed with and it was resolved to amend the Clause.

Clause 22

1. TESPOK proposal was disagreed with indicating that defining the term authorized personnel would unduly restrict the persons that may be authorized to conduct the investigations under the Bill.
2. Safaricom proposal was disagreed with noting that its inclusion as a requirement under the Clause would hamper execution of a validly obtained search warrant where the proposed 'Principal Officer' or person acting in a similar capacity in unavailable
3. Michael Odhiambo proposal on the need for the Bill to require investigating authorities to maintain the integrity and confidentiality of information seized while executing the search warrant.
4. KEPSA proposal was disagreed with noting that the term 'may' as used in the Clause adequately makes it mandatory for the police or authorized persons to obtain a warrant form the Court before conducting a search or a seizure under the Bill.

Clause 24

1. ISACA –Kenya, Article 19, TESPOK,ICTAK Michael Odhiambo. KEPSA.KICTANET memoranda sought deletion of the Clause arguing that there was no justification to conduct a search warrant and that the provision contradicts Article 24(2) and 31 of the Constitution.
2. TESPOK, CA, Ministry of ICT,CIPIT, Safaricom and KEPSA proposed that the clause be amended to outline the special circumstances in which a search could be conducted without search warrant. The Committee indicated that the special circumstances could include where the crimes being committed are of nature that does not allow investigative agencies. It was noted that there was need to amend the Clause to delete the erroneous references to the Criminal Procedure Code.

Clause 26

1. Committee disagreed with the KEPSA proposal noting that the term 'may' as used in the Clause adequately makes it mandatory for the police or authorized persons to obtain a production order for the Court before requiring the production of data or subscriber information for the purpose of investigations.
2. Safaricom Limited agreed with their proposal to the extent that disclosure of the existence of the production order is not likely to compromise any ongoing investigations.
3. KEPSA,ISACA-Kenya, Article 19, Safaricom Ltd, Media Council of Kenya, ICTAK CIPIT AND KICTANET proposal was agreed with, it was noted that there was need to delete the sub clause in order to require the police under the Act to seek permission form the Court before compelling the production of data or subscriber information.

MINUTE NO.057/2018: ADJOURNMENT

There being no other business, the sitting adjourned at 4.20 pm.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 15TH SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN WESTON HOTEL, NAIROBI ON FRIDAY 9TH MARCH 2018, AT 10.00 A .M.

PRESENT

1. Hon. William Kipkemoi, M.P. - **Chairperson**
2. Hon. George Macharia kariuki, M.P. - **Vice- Chairperson**
3. Hon. Annie Wanjiku Kibeh,M.P
4. Hon. Joshua Kimilu Kivinda, M.P.
5. Hon. Maritim Sylvanus, M.P.
6. Hon. Jonah Mburu, M.P.
7. Hon. Wamuchomba Gathoni, M.P.
8. Hon. John Kiarie Waweru, M.P
9. Hon. Godfrey Osotsi Atieno, M.P

APOLOGIES

1. Hon. Liza Chelule Chepkorir ,M.P
2. Hon. Marwa Kitayama Maisori, M.P.
3. Hon. Mwambu Mabongah, M.P.
4. Hon. Erastus Nzioka Kivasu, M.P.
5. Hon. Alfah O. Miruka, M.P.
6. Hon. Mwangaza Kawira, M.P
7. Hon. Anthony Tom Oluoch, M.P.
8. Hon. Gertrude Mbeyu Mwanyanje, M.P.
9. Hon. (Eng.). Mark Nyamita, M.P
10. Hon. Innocent Momanyi Obiri, M.P

IN ATTENDANCE

National Assembly Secretariat

1. Mr. Nicholas Emejen - Deputy Director, Committee Services
2. Ms.Ella Kendi - Third Clerk Assistant
3. Ms. Catherine Gati - Fiscal Analyst
4. Mr. Ronald Walala - Legal Counsel
5. Ms.Beatrice Auma - Secretary
6. Ms.Rahab Chepkilim - Audio officer
7. Mr. Wilson Angatangoria - Sergeant- at- arms

MINUTE NO. 050/2018: PRELIMINARIES

The Chairperson called the meeting to order at twenty minutes past ten o'clock followed with a word of prayer.

MINUTE NO.051/ 2018: CONFIRMATION OF MINUTES

The confirmation of the minutes of the previous sitting was deferred to the next meeting.

MINUTE NO.052/2018: CONSIDERATION OF THE SUBMISSION FOR THE COMPUTERS AND CYBERCRIME BILL, 2017

The Legal Counsel took the Members though the memoranda as follows;

Clause 11

1. ISACA proposal was rejected; It was pointed out that their proposal did not exist in the Bill. The Committee proposed the word 'Shillings' to be inserted after the word 'million'
2. Article 19 sought deletion of the Clause which the Committee disagreed with as the Clause restricts itself to the technological aspect of the espionage unlike the provisions of the Penal Code.
3. ICIPIT; the Committee agreed with the proposal of defining the term critical infrastructure.

Clause 12

1. ISACA-Kenya proposed reduction of the penalty which the Committee disagreed with the proposal noting that the fine prescribed proposes maximum penalty that allows the Court discretion on the sentences to impose under the Clause.
2. KICTANET proposed deletion and replacement of the Clause with a revised text. The Committee cited that the Clause failed to express the intention to limit the freedom of expression and the extent of the limitation as required by the Constitution. It was resolved to revise the Clause taking into consideration their proposal.

Clause 13.

1. Safaricom proposal was rejected as it was provided for in the Sexual and Offences Act. It was resolved to harmonize the Bill with the proposal by Kenya ICT Action Network and the Sexual Offences Acts to cover the offences not provided.
2. Media Council of Kenya, Information Communication Technology Association of Kenya, ICIPIT ISACA, KICTANET and Article 19 sought sought deletion of the Clause. The Committee rejected and resolved harmonization of the Bill with other Acts would resolve their concern.
3. Tespok proposal was disagreed with noting that Clause 32 of the Bill adequately indemnifies the service providers.

Clause 14

1. ISACA –Kenya and Article 19 proposals were rejected as the Clause covered the technological elements of forgery .It was resolved to harmonize the penalties with under the Clause with those under the Penal Code

Clause 15

1. ISACA Kenya proposal was agreed with indicating that there was need to harmonize the penalties under the Clause with those under the Penal Code.
2. KICTANET; the Committee disagreed with their proposal as the Penal Code does not provide for the offences committed through electronics. Their proposal was already provided for under Clause 21 of the Bill

Clause 16

1. ISACA – Kenya: The Committee disagreed with their proposal citing that that the issue of cyber harassment has become quite prevalent in the Country. That the seriousness of the offence and its potential impact on victim calls for the level of penalties provided for.

2. KICTANET and Medial Council of Kenya proposal was agreed with noting that cyber harassment covers the two aspects of cyber bullying and cyber stalking
3. Safaricom proposal was disagreed with noting that sub clause (3) (c) is a limited defence that applies only to law enforcement agencies.

Clause 17

Article 19, Media Council of Kenya and KICKANET proposal were disagreed with indicating that the offence of aiding and abetting under the Clause is limited to the offences under the Bill.

Clause 18

KEPSA and KICTANET proposals were disagreed with noting that the contents of the clause are clear as it deems offences upon corporations and its principal officers and prescribes penalties that only apply upon conviction of the officers charged.

MINUTE NO.053/2018: ADJOURNMENT

There being no other business, the sitting adjourned at 1.00 pm.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 14TH SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN 4TH FLOOR CONTINETAL HOUSE, PARLIAMENT BUILDINGS ON TUESDAY 1ST MARCH 2018, AT 11.30 A .M.

PRESENT

1. Hon. Kisang' William Kipkemoi, M.P. - **Chairperson**
2. Hon. Marwa Kitayama Maisori, M.P.
3. Hon. Mwambu Mabongah, M.P.
4. Hon. Wamuchomba Gathoni, M.P.
5. Hon. Erastus Nzioka Kivasu, M.P.
6. Hon. John Kiarie Waweru, M.P
7. Hon. Alfah O. Miruka, M.P.

APOLOGIES

1. Hon. George Macharia kariuki, M.P. - **Vice- Chairperson**
2. Hon. Liza Chelule Chepkorir ,M.P
3. Hon. Annie Wanjiku Kibeh,M.P
4. Hon. Joshua Kimilu Kivinda, M.P.
5. Hon. Mwangaza Kawira, M.P
6. Hon. Maritim Sylvanus, M.P.
7. Hon. Jonah Mburu, M.P.
8. Hon. Anthony Tom Oluoch, M.P.
9. Hon. Gertrude Mbeyu Mwananje, M.P.
10. Hon. (Eng.). Mark Nyamita, M.P
11. Hon. Innocent Momanyi Obiri, M.P
12. Hon. Godfrey Osotsi Atieno, M.P

IN ATTENDANCE

NATIONAL ASSEMBLY

1.	Mr. Nicholas Emejen	-	Deputy Director, Committee Services
2.	Ms. Catherine Gati	-	Fiscal Analyst
3.	Mr. Ronald Walala	-	Legal Counsel
4.	Mr. Sydney Lugaga	-	Legal Counsel
5.	Mr. Eugene Lutesh	-	Audio officer
6.	Mr. Wilson Angatangoria	-	Sergeant- at- arms

MINUTE NO. 045/2018: **PRELIMINARIES**

The Chairperson called the meeting to order at thirty minutes past eleven oclcok followed with a word of prayer.

MINUTE NO.046/ 2018: **CONFIRMATION OF MINUTES**

The confirmation of the minutes of the previous sitting was deferred to the next meeting.

MINUTE NO.047/2018: CONSIDERATION OF THE SUBMISSION FOR THE COMPUTER AND CYBERCRIMES BILL, 2017

(i) Article 19 proposal to delete the clause 5 was rejected The members further noted that it was important to amend the clause and include the term 'unauthorised persons'
(ii) The committee resolved that the submission by Article 19 to rephrase 'intentional' intent to 'dishonest' intent in Clause 6 be rejected.
(iii) The proposal by ISACA KENYA to reduce the penalty provided in Clause 7 of the Bill was rejected by the Committee.
(iv) It was resolved that the proposal by Article 19 to add serious physical injury' be rejected as the word 'serious' was too subjective.
(v) The Committee rejected the proposal by Safaricom to delete Clause 7

MINUTE NO.048/2018: ANY OTHER BUSINESS

The members were reminded of a retreat that would take place between 8th to 11th March 2018. The purpose of the retreat was to conclude the report on the Computer and Cybercrimes Bill, 2017. The committee resolved to hold the retreat in Mombasa to take place after the Post-Election Seminar organised by CPA and the National Assembly.

MINUTE NO.049/2018: ADJOURNMENT

There being no other business, the sitting adjourned at 1.30 pm. Next sitting of the committee was to be communicated by the secretariat in due course.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 13TH SITTING OF THE COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN 4THFLOOR, CONTINENTAL HOUSE, PARLIAMENT BUILDINGS ON TUESDAY 27TH FEBRUARY 2018 AT 11.30 A.M.

PRESENT

1. Hon. Kisang' William Kipkemoi, M.P. - **Chairperson**
2. Hon. Marwa Kitayama Maisori, M.P.
3. Hon. Mwangu Mabongah, M.P.
4. Hon. Wamuchomba Gathoni, M.P.
5. Hon. Erastus Nzioka Kivasu, M.P.
6. Hon. Anthony Tom Oluoch, M.P.

APOLOGIES

1. Hon. George Macharia kariuki, M.P. - **Vice- Chairperson**
2. Hon. Liza Chelule Chepkorir ,M.P
3. Hon. Annie Wanjiku Kibeh,M.P
4. Hon. Alfah O. Miruka, M.P.
5. Hon. Joshua Kimilu Kivinda, M.P.
6. Hon. Mwangaza Kawira, M.P
7. Hon. Maritim Sylvanus, M.P.
8. Hon. Jonah Mburu, M.P.
9. Hon. Gertrude Mbeyu Mwananje, M.P.
10. Hon. (Eng.). Mark Nyamita, M.P
11. Hon. John Kiarie Waweru, M.P
12. Hon. Innocent Momanyi Obiri, M.P
13. Hon. Godfrey Osotsi Atieno, M.P

IN ATTENDANCE

National Assembly

1. Mr. Nicholas Emejen - Deputy Director, Committee Services
2. Ms. Catherine Gati - Fiscal Analyst III

MINUE NO.041/2018: PRELIMINARIES

The Chairperson called the meeting to order at 12.26 pm and thereafter welcomed all the members present. A prayer was said.

MINUTE NO.042/2018: CONFIRMATION OF MINUTES

Confirmation of the minutes of the previous sitting was deferred to the next meeting.

MINUTE NO.043/2018: PENDING BUSINESS BEFORE THE COMMITTEE

The Chairperson informed the Committee that –

(i) The Computers and Cybercrimes Bill, 2017 and the Copy right amendment bill was still before the committee. The Committees report on the Bill is long overdue.

(ii) Due to the nature of the Computers and Cybercrimes Bill, 2017 and a request by the Chairperson of the Departmental Committee on Administration and National Security, a joint meeting will be held on Thursday 1st March, 2018 in order to jointly discuss and make deliberations regarding the Bill.

The Committee noted that a report on the bill is required in the House and as such there was need to undertake a report writing retreat to conclude on its consideration. The Committee resolved to undertake a report writing retreat in Mombasa from 8th to 11th March, 2018 in Mombasa (Hotel to be confirmed) to finalize and adopt the report on the Computer and Cybercrimes Bill, 2017.

MINUTE NO.044/2018: ADJOURNMENT

There being no other business, the sitting adjourned at 1.00pm.Next sitting of the committee to be held on Thursday 1St March 2018 on 4th Floor in Continental House, Parliament Buildings.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 12TH SITTING OF THE COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD ON MONDAY 26TH FEBRUARY 2018 IN COMMITEEE ROOM 9, MAIN PARLIAMENT BUILDINGS AT 10.00 A.M.

PRESENT

1. Hon. Kisang' William Kipkemoi, M.P. - **Chairperson**
2. Hon. Marwa Kitayama Maisori, M.P.
3. Hon. Mwambu Mabongah, M.P.
4. Hon. Erastus Nzioka Kivasu, M.P.
5. Hon. John Kiarie Waweru, M.P
6. Hon. Anthony Tom Oluoch, M.P.
7. Hon. Jonah Mburu, M.P.
8. Hon. Godfrey Osotsi Atieno, M.P

APOLOGIES

1. Hon. George Macharia Kariuki, M.P. - **Vice- Chairperson**
2. Hon. Liza Chelule Chepkorir ,M.P
3. Hon. Annie Wanjiku Kibeh, M.P
4. Hon. Alfah O. Miruka, M.P.
5. Hon. Joshua Kirnilu Kivinda, M.P.
6. Hon. Mwangaza Kawira, M.P
7. Hon. Maritim Sylvanus, M.P.
8. Hon. Gertrude Mbeyu Mwananje, M.P.
9. Hon. (Eng.) Mark Nyamita, M.P
10. Hon. Innocent Momanyi Obiri, M.P
11. Hon. Wamuchomba Gathoni, M.P.

IN ATTENDANCE

NATIONAL ASSEMBLY

1. Mr. Nicholas Emejen - Deputy Director, Committee Services
2. Mr. Ronald Walala - Legal Counsel

MIN No. 036/2018: PRELIMINARIES

The Chairperson called the meeting to order at 10.30 am and thereafter welcomed all the members present. A prayer was then said.

MIN No. 037/ 2018: CONFIRMATION OF MINUTES

The confirmation of the minutes of the previous sitting was deferred to the next meeting.

MIN No. 038/2018: MEETING WITH KICTAnet

The committee held a meeting with members of the Kenya ICT Action Network (KICTAnet) who presented a memorandum on the Computer and Cybercrimes Bill, 2017. The group led by the Co-Convener Grace Githaiga, presented a written memoranda and made oral submissions as per the attached memoranda.

The Committee received the submissions and resolved to consider them in details during the report writing retreat.

MIN No. 039/2018: MEETING WITH VISITING UGANDAN DELEGATION

The Committee held a meeting with a visiting delegation comprising of members of Parliament and staff from the Parliament of Uganda. The delegation was on a benchmarking visit on the local content policy in Kenya. The delegation comprised of –

1. Hon. Patrick Nsamba, MP – Leader of delegation
2. Hon. Norah Bigiriwa, MP
3. Hon. Anna Adeke, MP
4. Hon. Herbert Ariko, MP
5. Hon. Maurice Kibaiya, MP
6. Mr. john Tamale – Legal Counsel
7. Mr. Max Komakech - Principal Clerk

The Committee discussed local content policy as it relates to the ICT sector.

MIN No. 040/2018: ADJOURNMENT

There being no other business, the sitting adjourned at 1.00pm. Next sitting of the Committee to be held on Tuesday 27th February, 2018 on 4th Floor in Continental House, Parliament Buildings at 11.30 am.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 11TH SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN FOURTH FLOOR PROTECTION HOUSE ON FRIDAY 23RD FEBRUARY, 2018 AT 10.00AM

PRESENT

1. Hon.Kisang William Kipkemoi, M.P — **Chairperson**
2. Hon.George Kariuki, M.P — **Vice-Chairperson**
3. Hon.Wamuchomba Gathoni, M.P
4. Hon.Joshua Kimilu Kivinda, M.P.
5. Hon.Gertrude Mbeyu Mwanyanje, M.P.
6. Hon.John Kiarie Waweru, M.P.
7. Hon.Anthony Tom Oluoch, M.P.
8. Hon.(Eng)Mark Nyamita Ogola,M.P
9. Hon.Jonah Mburu, M.P.
10. Hon.Liza Chelule Chepkorir, M.P.
11. Hon.Mwambu Mabongah, M.P.
12. Hon.Annie Wanjiku,M.P.
13. Hon.Maritim Sylvanus, M.P.

APOLOGIES

1. Hon.Innocent Momanyi Obiri, M.P
2. Hon.Erastus Nzioka Kivasu, M.P.
3. Hon.Godfrey Osotsi Atieno , M.P
4. Hon.Mwangaza Kawira, M.P.
5. Hon.Alfah Miruka, M.P.
6. Hon.Marwa Kitayama Maisori, M.P.

IN ATTENDANCE

National Assembly Secretariat

1. Mr.Ronald Walala	Legal Counsel II
2. Ms.Catherine Gati	Fiscal Analyst
3. Ms.Lorna Okatch	Research Officer III
4. Mr.Wilson Antangangoria	Sergeant at arms

Ministry of ICT

1.	Mr.Joe Mucheru	Cabinet Secretary
2.	Mr.Sammy Itemere	Principal Secretary
3.	Carolina Thuku	P.A to CS
4.	Maina Magama	Information Secretary
5.	Mr.Christopher Maina	Legal Officer
6.	Mr.Vincent Ngundi	Assistant Director
7.	Ms.Mercy Wanjau	Principal Legal Officer.
8.	Mr.David Jakaiti	Secretary Administration

MINUTE NO. 033/2018 PRELIMINARIES

The meeting was called the meeting to order at twenty minutes past ten o'clock followed with a word of prayer and thereafter introductions.

MINUTE NO.034/2018 CONFIRMATION OF THE MINUTES

Confirmation of the minutes of the was deferred to the next meeting.

MINUTE NO.034/2018 CONSIDERATION OF THE COMPUTERS AND CYBCERCRIMES BILL, 2017

Mr.Joe Mucheru, the Cabinet Secretary appeared before the Committee and informed them as follows;

Emerging technologies have enabled numerous functionalities and led to a heavy reliance on ICTs in our daily lives.However heavily dependence on technology has various challenges including;

1. Emergence of the Cybercriminal
2. False publications aka fake news
3. Cyber bullying/stalking
4. Cyber espionage
5. Child pornography
6. Computer forgery

The Cabinet Secretary presented their memoranda as follows;

1. In the preliminary section the Bill makes reference to the Mutual Legal Assistance Act and no mention of the Extradition (Contiguous & Foreign Countries) Act

Justification:
Both the Mutual Legal Assistance Act and the Extradition (Contiguous & Foreign Countries) Act are complementary in ensuring the successful prosecution of offences under this proposed law.

2. **Section 2 – Interpretation**

Inclusion of new definitions for key terms used in the Bill for "critical national information infrastructure" and "critical data"

Justification: "**critical national information infrastructure**" means a computer or a computer system that is necessary for the continuous delivery of essential services which Kenya relies on, the loss or compromise of which will lead to a debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Kenya;

3. **Section 24(1) on** power to search without a warrant in special circumstances

Define criteria for situations that would meet the threshold for 'special circumstances

Justification: Waiver for the requirement for a warrant in advance of undertaking a search has the huge potential of infringing on constitutional rights an liberties, hence the need to be achieve with clarity circumstances under which this requirement would be waived in order to provide a an objective framework within which to evaluate applications.

S. 24(2) – Section 119, 120 and 121 of the Criminal Procedure Code cited to serve as guidance are very removed from the reality of the speed and sophistication attendant to cybercrime and may need to be infused with this reality.

4. **Section 41**

Delete 'and prosecuting cybercrime' from the third line as it creates a conflict of interest.

Justification: The point of contact should be the investigating agency only in order to promote independence of roles.

General Comment

The success of implementation of this draft law will rest on a number of institutions, among them the NPS, NIS, CA, ICTA, KDF, ODPP etc.
There is need to formalize a collaboration, and identify an appropriate agency empowered to handle the key elements of this law particularly the mutual legal assistance aspect.
Following the presentations, it was observed that;

1. For enforcement purposes of this Bill, it was pointed out that there need for establishment of an enforcement Authority to handle the issue of Computer and Cybercrime and this will have financial implication.

2. There was need to harmonize the Sexual Offences Act with Clause 13 of the Bill to avoid contradiction.

3. Clause 24 and 26(6) of the Bill allows for searches without warrant under special circumstances and obtaining subscriber information without a court order. It was

noted that the right to privacy is not absolute and can be limited in within specific limits in accordance with Article 24 of the Constitution.

4. The amount of fines and terms of imprisonment proposed in the Bill had been harmonized taking into consideration the various Acts of Parliament and other jurisdiction.

MINUTE NO. 035/2018 ADJOURNMENT

There being no other business, the meeting was adjourned at 12.00p.m.

Signed.....

(Chairperson)

Date.....19/03/2018.....

MINUTES OF THE 4TH SITTING OF THE DEPARTMENTAL COMMITTEE ON COMMUNICATION, INFORMATION AND INNOVATION HELD IN BOARD ROOM, 11TH FLOOR, PROTECTION HOUSE, PARLIAMENT BUILDINGS ON THURSDAY 15TH FEBRUARY 2018 AT 10.00AM.

PRESENT

1. Hon. Kisang William Kipkemoi, M.P — **Chairperson**
2. Hon. George Kariuki, M.P — **Vice-Chairperson**
3. Hon. Alfah Miruka, M.P.
4. Hon. Annie Wanjiku, M.P.
5. Hon. Joshua Kimilu Kivinda, M.P.
6. Hon. Marwa Kitayama Maisori, M.P.
7. Hon. Mwambu Mabongah, M.P.
8. Hon. Maritim Sylvanus, M.P.
9. Hon. Anthony Tom Oluoch, M.P.
10. Hon. (Eng)Mark Nyamita Ogola, M.P
11. Hon. Innocent Momanyi Obiri, M.P.
12. Hon. Godfrey Osotsi Atieno, M.P
13. Hon. Mwangaza Kawira, M.P.
14. Hon. Jonah Mburu, M.P.
15. Hon. Gertrude Mbetu Mwanyanje, M.P.
16. Hon. John Kiarie Waweru, M.P.
17. Hon. Erastus Nzioka Kivasu, M.P.
18. Hon. Wamuchomba Gathoni, M.P
19. Hon. Liza Chelule Chepkorir, M.P.

IN ATTENDANCE

National Assembly Secretariat

1.	Ms. Ella Kendi	Third Clerk Assistant
2.	Mr. Ronald Walala	Legal Counsel II
3.	Ms. Lorna Okatch	Research Officer III
4.	Mr. Wilson Angatangoria	Serjeant at Arms
5.	Mr. Collins Mahamba	Audio Officer

MINUTE NO. 009/2018 PRELIMINARIES

The meeting was called to order at ten minutes past ten followed with a word of prayer.

MINUTE NO.010/2018 CONFIRMATION OF THE MINUTES

Minutes of the 2nd sitting of the Committee were confirmed as true record of the proceedings having been proposed by Hon. Marwa Maisori, MP and seconded by Hon. Mwambu Mabongah, MP.

MINUTE NO.011/2018 MATTERS ARISING

Under the heading the dates to be corrected to read 8th February, 2018

MINUTE NO.012/2018 CONSIDERATION OF THE COMPUTERS AND CYBERCRIME BILL, 2017

The Legal counsel took the Members through Part I and Part II of the Bill. The Members were informed as follows -

The Bill seeks to provide for offences relating to computer systems in order to enable timely and effective detection, investigation and prosecution of computer and cybercrimes, including in collaboration with other states under mutual legal assistance agreements. In particular—

(a) **Clause 2** of the Bill contains the definition of terms used in the Act. The responsible Cabinet Secretary for the Act is defined as the Cabinet Secretary responsible for matters relating to Information, Communications and Technology.

(b) **Clause 3** outlines the objects of the Bill as the protection of the confidentiality, integrity and availability of computer systems, programs and data; prevention of the unlawful use of computer systems; facilitation of investigation and prosecution of cybercrimes; and facilitation of international cooperation on the subject matter of the Bill.

Part II of the Bill outlines the various offences proscribed under the Bill. These are—

(i) Unauthorized access of a computer system which is punishable with the imposition of a fine not exceeding five million shillings or a term of imprisonment not exceeding three years, or both;

(ii) Access of a computer system with intent to commit or facilitate the commission of a criminal offence which is punishable with the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding ten years, or both;

(iii) Unauthorized interference with a computer system, program or data which is punishable with the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both. Where the interference results in a significant financial loss to a person, threatens national security, causes physical injury or death to a person or threatens public health or public safety, the penalty is enhanced to a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(iv) Unauthorized interception of data to or from a computer system over a telecommunication system which is punishable with the imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(v) Manufacture, adaptation, sale procurement for use, importation, offering to supply, distribution or otherwise making available for use a device, program, computer password, access code or similar data for the purpose of committing an offence under the Bill which is punishable with the imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding five years, or both. A person who without sufficient justification receives a device, program, computer password, access code or similar data for the purpose of committing an offence under the Bill also commits an offence punishable with the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both;

(vi) Unauthorized disclosure of a password, access code or other means of gaining access to a program or data held in a computer system which is punishable with the imposition of a fine not exceeding five million shillings or a term of imprisonment not exceeding three years, or both. Where the disclosure is intended for a wrongful gain, an unlawful purpose or to occasion any loss, the penalty is enhanced to the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both;

(vii) Unauthorized access, interference with or interception of data to or from a protected computer system which is punishable with the imposition of a fine not exceeding twenty five million shillings or a term of imprisonment not exceeding twenty years, or both;

(viii) Cyber espionage which is punishable with the imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding twenty years, or both;

(ix) Publishing false, misleading or fictitious data with the intention that the data be considered or acted upon as authentic which is punishable with imposition of a fine not exceeding five million shillings or a term of imprisonment not exceeding two years, or both;

(x) Publication, production or possession of child pornography on a computer system which is punishable with imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding twenty five years, or both;

(xi) Forgery of computer data resulting in inauthentic data with the intention that the data be acted upon for legal purposes as if authentic which is punishable with imposition of a fine not exceeding ten million shillings or a term of imprisonment not exceeding five years, or both. Where the forgery is intended for wrongful gain, wrongful loss to another person or economic benefit, the penalty is enhanced to a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(xii) Cyberstalking and cyberbullying which are punishable with imposition of a fine not exceeding twenty million shillings or a term of imprisonment not exceeding ten years, or both;

(xiii) Aiding or abetting the commission of an offence under the Bill which is punishable with imposition of a fine not exceeding seven million shillings or a term of imprisonment not exceeding four years, or both;

(xiv) Commission of an offence under the Bill by a body corporate punishable with imposition of a fine not exceeding fifty million shillings to the body and a fine not exceeding five million shillings or a term of imprisonment not exceeding three years, or both on the principal officer of the body;

(xv) Commission of an offence provided for under any other law through a computer system which is punishable with, in addition to the penalty provided under that law, imposition of a fine not exceeding three million shillings or a term of imprisonment not exceeding four years, or both.

Following the presentations, the following observations were made;

1. Clause 12 of the Bill which provides for false publication contradicts freedom of expression granted under the Constitution.
2. The fines provided in the Bill for various offences committed, contradicts with various existing Acts eg the Election Offences Act and Sexual Offences Act. There was need to harmonize the Bill with other Acts to ensure consistency.
3. Clause 13 which provides for child pornography offences was dealt with under Sexual Offences Act (2006) hence the Bill should be aligned with the Act.
4. There was need for clarification from the Ministry of ICT on the criteria used to determine the amount of fine charged under each offence committed.
5. Clause 16 which provides for cyber bullying and Cyber stalking to be revamped to cover the crimes committed using anonymous accounts on social media platforms causing individuals untold suffering.
6. It was noted that the Security departments do not have the capacity and technology needed to deal with cyber security hence there was need for the Ministry of ICT to establish a body with highly trained personnel to deal with cyber security issues.

MINUTE NO. 013/2018 ADJOURNMENT

There being no other business, the meeting was adjourned at 12.20pm

SIGNED.....

(Chairperson)

DATE.....19/03/2018.....

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

44

(1) D/Clerk 14/2/18

The Clerk of the National Assembly,
P. O. Box 41842 - 00100, Nairobi
13th February 2018

(2) Engrossed pls deal FA 14/2/18

ISACA KENYA MEMORANDUM ON THE COMPUTER AND CYBERCRIMES BILL, 2017

ISACA Kenya welcomes the bill on computer and cybercrimes whose purpose is to enable timely and effective detection, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for connected purposes

Following our review, ISACA Kenya proposes the following amendments to the bill.

SECTION	AMENDMENT	RECOMMENDATION/ COMMENT
Section 2 In this Act, unless the context otherwise. requires—	Section 2 of the Computer and Cybercrimes Act, 2017 be amended(a) In subsection (2) by inserting the following definitions: "Confidentiality" means preserving authorized restrictions on information	Define the term confidentiality, integrity and availability as they are defined as objects of this Act under Section 3.

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384–00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

	access and disclosure, including means for protecting personal privacy and proprietary information "Integrity" means Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. "Availability" means ensuring timely and reliable access to and use of information	
7. (1) A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.	Section 7 of the Computer and Cybercrimes Act, 2017, be amended by deleting the words "ten million shillings or to imprisonment for a term not exceeding five years, or to both" after the words "not exceeding" and substituting therefor the words "five million shillings or to imprisonment for a term not exceeding three years, or to both"	The fine for interception should be lower than interference. This is because interference is a more serious offense than interception. The fine should be halved to five million and an imprisonment of 3 years.

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

8) A person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer system commits an offence and is liable, on conviction, to a fine not exceeding five million shillings or to imprisonment term for a term not exceeding three years, or to both.	Section 8 of the Computer and Cybercrimes Act, 2017, be amended by deleting the words "five million shillings or to imprisonment term for a term not exceeding three years, or to both" after the words "not exceeding" and substituting therefor the words "one million shillings or to imprisonment for a term not exceeding one year, or to both"	The fine for disclosing a password is too punitive. It should be lower as many people as still sharing passwords.
10. (1) Where a person commits any of the offences specified under sections 4, 5, 6 and 7 on a protected computer system, that person shall be liable, on conviction, to a fine not exceeding twenty five million shillings or imprisonment term not exceeding twenty years or both. (2) For purposes of this section—	Section 10 of the Computer and Cybercrimes Act, 2017, be amended by Deleting subsection 2(c)	(a) By including a system that is "necessary for the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically" as protected system enlarges the scope of a

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

"protected computer system" means a computer system used directly in connection with, or necessary for, (a) the security, defence or international relations of Kenya: (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically; (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services; (e) the provision of national registration systems; or (f) such other systems as may be designated by the Cabinet Secretary in		protected system to virtually any computing system. Most of these systems are run privately and we don't disagree with it being classified as a protected system.

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

the manner or form as the Cabinet Secretary may consider appropriate		
11. (3) A person who unlawfully and intentionally performs or authorizes, or allows another person to perform a prohibited act as envisaged under this Act in order to gain access, as provided under section 4 to or intercept data as provided under section 7, which is in possession of the State and which is exempt information in accordance with the law relating to access to information, with the intention to directly or indirectly benefit a foreign state against the Republic of Kenya, commits an offence and is liable, on conviction, to a fine not exceeding five million or to imprisonment for a period not exceeding ten years or to a fine not exceeding five million, or to both.	Section 11 of the Computer and Cybercrimes Act, 2017, be amended by deleting the words "to a fine not exceeding five million" after the words "ten years"	This is a repetition.
12. 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	Section 12 of the Computer and Cybercrimes Act, 2017, be amended by deleting the words "five million shillings or to imprisonment term for a term not exceeding two years, or to both" after	While false publication is becoming a challenge in an era of "fake news" we believe that this fine is too prohibitive and especially in cases that might infringe on

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384–00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

imprisonment for a term not exceeding two years, or to both.	the words "not exceeding" and substituting therefor the words "one million shillings or to imprisonment for a term not exceeding one year, or to both"	creativity and restriction on freedom of expression.
13. Child Pornogrqphy	Section 13 of the Computer and Cybercrimes Act, 2017, be amended by deleting the entire Section AND updating the Sexual Offenses Act Appropriately.	Child Pornography is covered under the Sexual offenses Act. We don't see a justification for it to be in this bill. Furthermore, Section 21 of this bill, provides for additional penalties for any offense committed through any other law and with the use of computer system. This is quoted as "A person who commits an offence under any Offences committed other law, through the use of a computer system, is liable through the use of on conviction, in addition to the penalty provided under a computer that law to a fine not exceeding three million shillings or to a imprisonment

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

		term for a term not exceeding four years, or to both."
Section 14 and 15	The penalties should be harmonized with the penal code	
16. (1) A person who, individually or with other persons, willfully 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. (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.	Section 16 of the Computer and Cybercrimes Act, 2017, be amended by deleting the words "twenty million shillings or to imprisonment term for a term not exceeding ten years, or to both" after the words "not exceeding" and substituting therefor the words "one million shillings or to imprisonment for a term not exceeding one year, or to both"	While Cyberbullying is a serious offense, we believe that the penalties are too prohibitive and should be lowered.
24 **Powers to search without a warrant in special circumstances**	Section 24 of the Computer and Cybercrimes Act, 2017, be amended by deleting the entire Section	There is no justification to search without a warrant. Furthermore the sections mentioned on the criminal procedure code on searching without a warrant do not exist.

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

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.	Section 26 of the Computer and Cybercrimes Act, 2017, be amended by deleting section 26(6)	We believe that at all times, judicial oversight should be available for any access to subscriber information.
27 (2) The data specified in the notice shall be preserved and its integrity shall be maintained for a period not exceeding the period specified in the notice.	Section 27 of the Computer and Cybercrimes Act, 2017, adding the "30 days" so as to read (2) The data specified in the notice shall be preserved and its integrity shall be maintained for a period not exceeding **30 days** ~~the period specified in the notice.~~	30 days is enough and provides a definitive guide in preservation of traffic data.
28 (4) For purposes of subsection (1), real-time collection or recording of traffic data	Section 28 of the Computer and Cybercrimes Act, 2017, be amended by deleting the word "six" after the	Preservation of real-time data for six months is an expensive task. We believe that 3 months should suffice and in any case an

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

shall not be ordered for a period not exceeding six months.	words "not exceeding" and substituting therefor the word "one"	extension can be granted if sufficient need arises.
Governance Framework	We request an addition of a section on the Computer and Cybercrimes Act, 2017 include a section on governance framework which can be stated as: "The Cabinet Secretary to form a governance council, a body to be charged with provision on guidance, training and overall implementation of this Act. The body should consist of players from both the public and private sector, professional association bodies that are involved in cybersecurity, information security or cybercrime"	Due to the evolution of cybercrime, and cyber-attacks, we propose a multisectoral approach to ensure that the country is well prepared to detect, investigate and prosecute cybercrime. At the moment, most of our infrastructure, training and prosecution is not digital ready. This body will ensure that • It provides a governance framework for prosecution of cybercrime while also taking into consideration privacy and protection of individual rights • Provides a mechanism of transitioning our police officers, prosecutors, judicial offers and other authorized persons to a digital ready arena through training, awareness sessions and general guidance • Monitor attacks through a CERT (Computer Emergency Readiness Team) which can be regulated and provide for a defense mechanism before such crimes are committed.

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

		• Allow for information sharing on cyber-attacks to various bodies • Provide for a mechanism for disclosure of breaches and notifications to affected parties.

Yours Faithfully,

Preston Odera
Chief Executive Officer (CEO)
ISACA Kenya Chapter

About ISACA

ISACA Kenya ("The Chapter") is a not-for-profit, non-union association of professionals in the IT-related industry founded in Kenya in December 1999 by a small group of volunteers. The chapter was locally registered in Kenya in April 2000 and has since experienced tremendous growth in membership, once earning global recognition for achieving the second highest annual percentage growth ir membership worldwide.

ISACA®
Trust in, and value from, information systems
Kenya Chapter

Vision Plaza
3rd Floor, Suite. 4
Mombasa Road
P.O Box 10384– 00100,
Nairobi Kenya

Phone: +254205100001
Mobile: +254 (786) 249357
Mobile: +254 (717) 116518
Email: admin@isaca.or.ke
Web: www.isaca.or.ke

ISACA Kenya currently has more than 1,300 members drawn from the fields of IT audit, risk management, information security and IT governance. ISACA Kenya is one of more than 200 local chapters in more than 180 countries affiliated to ISACA international, a leading information technology association of individual members.

REVISED MEMORANDUM ON PROPOSALS FOR AMENDMENT OF THE COMPUTER AND CYBERCRIMES BILL 2017

Submitted to the National Assembly by the Kenya ICT Action Network (KICTANet)

February 2018

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. Add definition of "authorised person" "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; "critical infrastructure" means vital virtual	These were previously included in the body of the Bill. They are better placed in the definition clause 2.

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	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

		found in possession of data, with the knowledge that such data was acquired unlawfully as contemplated in subsection (1), is guilty of an offence.	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 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 (1) which,— results in a significant financial loss to any person; threatens national security;	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 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.	Revision is intended to make the provision concise and define what interference constitutes. Recently, cases of people developing Bots, Malware, Ransomware are becoming common.

	(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.		
8	Illegal devices and access codes 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	Amend section Insert the words "rents, transfers," immediately after "sells" Insert the words "as a means of access or control" immediately before the word "designed" Illegal devices and access codes	The provision should also prohibit the rent or transfer of devices or programmes including such other means of access or control of computers to commit offences. This is especially relevant to tackling the use of botnets for criminal activity.

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.	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.

	(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— (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	Delete provision	Fraud is already provided for

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.
(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

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; 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

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—	(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	

(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.	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.	

	(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.		
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	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	seems clearer as paraphrased

1. Proportionality:
2. Equality / Uniformity / Parity / Consistency / Impartiality
3. Accountability/Transparency
4. Inclusiveness
5. Respect for Human Rights and Fundamental Freedoms
6. Adherence to domestic and international law with due regard to recognised international and regional standards on sentencing

		(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; 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	Delete Provision	The provision does not fit the test provided under Article 24(2)

	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.		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	Delete entire sub-section (6)	The provision violates the right To privacy. It lowers the

	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.		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	Delete provision	This provision flies in the face of the right to privacy as enshrined under Article 31 of the

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 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

Constitution, which provides inter alia that:

Every person has the right to privacy, which includes the right not to have—

(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.

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-
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.

33,34	Part Iv-International cooperation		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. There needs to be adequate assessment of regional

In Korea there is KICS (Korea Information System of Criminal justice system which is an electronic work system by which the four criminal justice agencies (police, prosecution service, courts, and the Ministry of Justice) perform investigation, indictment, trial, and execution work through the standard information system, and jointly use the resulting information and other documents. with these format

(2) In korea there Digital forensic Technical manual 2017.

(3) The is importance of the responding officer to be well-trained person with specialised investigative role, who are then singularly capable of closing many cases rather than turning them over to another person (Block & Weidman, 1975; Greenberg, Elliot, Kraft, & Proctor, 1977).

		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.	
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 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.	Any limitation of rights under the Constitution, is subject to Article 24 and as such must be expressly provided for by Statute
New clause		Insert new clause Online Grooming	This is becoming an issue for concern in the country and needs to be addressed. This is

	(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 all the circumstances but regardless of any person's purpose, consider to be sexual.	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.
New Clause	Insert new clause	This is becoming an issue for concern in the country and

		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.	needs to be addressed. https://www.pri.org/stories/2016-12-08/child-sex-trade-booming-kenyan-port-city
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. https://www.capitalfm.co.ke/business/2017/05/bank-fraudsters-focus-customer-identity-theft-kba/ https://www.nation.co.ke/news/Banks-Fraud-Technology-/1056-2446010-aq7r4qz/index.html

New Clause	Insert new clause Cyber Squatting	This is becoming an issue for concern in the country that needs to be addressed. https://www.businessdailyafrica.com/magazines/Cybersquatters-hit-e-commerce-/1248928-1498082-c0ii7kz/index.html

		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.	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	This is for the ODPP to include cybercrime in its annual report.
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	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

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.	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.	
False publications	Amend provision and substitute with the following 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 commits an offence if the publication amounts to– (a) propaganda for war; (b) incitement to violence; (c) hate speech; or (d) advocacy of hatred that– (i) constitutes ethnic incitement, vilification of others or incitement to cause harm; or (ii) is based on any ground of discrimination specified or contemplated in Article 27(4) of the Constitution.	This provision constitutes an unjustifiable limit on the right to freedom of expression and opinion granted under the constitution. The UN Special Rapporteur & the UN Human Rights Committee have deemed such provisions unacceptable. The limits of the right are provided under Art. 33(2) of the Constitution. 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

		(10) Applications under this section must be resolved expeditiously and in any case within fourteen days of filing of the complaint. (11) If the Court is satisfied that a restraining order must be issued to protect the complainant from harassment by electronic means and the identity of the respondent is unknown, the court may require an internet service provider to furnish the court with any information that is available to the internet service provider which may be of assistance to the court to identify the respondent or the internet service provider which provides service to the respondent. (12) 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 willfully 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.	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.

chain of custody. these is particularly important since First, the role the responding officer is crucial in investigations, and oftentimes the information provided to him or her is the deciding factor in solving a case.

The role of the first responding law enforcement officer in computer crime
cases is of critical import because the evidence associated with a compute
r crime is often intangible in nature. Certain precautions must be taken to ensure that data stored on a system or on removable media is not modified or deleted -either intentionally or accidentally (Lyman, 2002; Parker, 1976). Even the simple shutting-down of a computer can change the last-modified or last-accessed timestamp of certain system files, which introduces questions associated with the integrity of the data.

MODERN APPLICATION

sources. Investigators (Police officer and or Authorised person have to understand the characteristics and develop the sources evidence collection before applying court order. These may pose as a challenge since due to silent nature of computer crime and hidden electronic evidence. These can be solved by having integrated system where court, police, authorised and judiciary can have real time identification and judicial order application systems with online recording of the chain of custody.

(2) To overcome the challenges of evidence collection,we propose the formulating Digital Forensics Technical Manual which should be applicable digital evidence collecting situations concerning computer systems and peripherals

(3) There is need to specify that the police officer should be trained in cyber forensics or work with help of authorised cyber forensics to be able secure the evidence at crime scene and maintains the

			instruments to compare and contrast with the bill. (KICTANet was not able to do that within this short period of public consultation).
	38. A police officer or another authorised person may, without the authorisation but subject to any applicable provisions of this Act— access publicly available (open source) stored computer data, regardless of where the data is located geographically; or	Delete the phrase "(Open source)"	

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	It is important to have a clear standard procedure for the collection of electronic evidence by law enforcement agencies. Whereas Investigation generally begins by gathering initial information from a variety of

	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, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years, or to both.	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	
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.	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 criteria for aggravating factors to be considered when charges/sentences are enhanced. Principles underpinning Sentencing

(5)A restraining order is an order prohibiting the respondent from–

(a) engaging or attempting to engage in harassment;

(b) enlisting the help of another person to engage in harassment; or

(c) committing any other act specified in the restraining order.

(6) An application under this section may be instituted by–

(a) a complainant acting in their own interest; or

(b) Any other person who has a material interest in the well-being of the complainant.

(6) Notwithstanding the provisions of any other law, a child may apply to the court for a restraining order without the assistance of a parent or guardian.

(7) An application under this Section may be made outside court working hours.

(8) The court may grant a restraining order outside court working hours where there is reason to believe that the complainant is suffering or may suffer harm if the order is not granted immediately.

(9) The court may grant an ex parte interim restraining order pending the hearing and final determination of the complaint.

	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.		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. (2) A person who commits an offence under subsection (1) is liable, on conviction, to a fine not exceeding twenty million shillings or	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— (a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that persons' property;	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. See: Cyber harassment in the UK: https://www.cps.gov.uk/legal-guidance/stalking-and-harassment Cyber misbehaviour in US - https://www.justice.gov/usao/file/851856/download

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.

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.

The Clause has been amended to reflect the exceptions to Freedom of Expression allowed by Article 33 of the Constitutions.
The offence can be dealt with under s.13 of National Cohesion and Integration Act hate speech and under Civil defamation. The provision if retained is like to be challenged in court as the following:

Andare v. AG (2016) - Declared s.29 of KICA unconstitutional - https://globalfreedomofexpression.columbia.edu/cases/andare-v-attorney-general/

Okuta v. AG (2017) - Declared

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.

s.194 of Penal Code unconstitutional - https://globalfreedomofexpression.columbia.edu/cases/okuta-v-attorney-general/

See the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda for a global position on such legislative provisions. https://www.article19.org/resources/joint-declaration-on-freedom-of-expression-and-fake-news-disinformation-and-propaganda/

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.

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) advice 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

	i) conduct research and surveys to inform the country's approach to cyber security.	
New	Insert New clause Functions of the Communications Authority in relation to Cybersecurity (1) The Authority shall ensure a co-ordinated, efficient, effective and consultative approach in the coordination of cybersecurity initiatives, including at the counties. (2) To achieve the objectives set out under subsection (1), the Authority 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. 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	

	(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 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.	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 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. 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

	the offences. (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	It is important to establish a multi-stakeholder body to review and coordinate the actions by state and non-state actors on cybersecurity. This is the emerging best practice. Other State with similar agency include. South Africa which created the National Cybersecurity Advisory Council, https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/NCAC-ToR-2017-Reappointment_V1.pdf Ghana has it as Ghana National Security Council

		(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 -	This is becoming an issue for concern in the country and needs to be addressed.[1]

[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

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 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	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

	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.	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 (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	This is proposed so as to deal with persons or organizations who are reckless or knowingly trading or sharing personal data collected by them in trust for purposes other than which was intended.

		(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.	
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, including where the data is held by the state.	This is to ensure the creation of a policy and legal framework for the protection of personal information.

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	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.

https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Ghana_Cyber-Security-Policy-Strategy_Final_0.pdf

Mauritius calls it the Mauritius CyberSecurity Committee.
https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Ghana_Cyber-Security-Policy-Strategy_Final_0.pdf

EU - National Cybercrime Centre - https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
UK - National Cyber Security Centre - https://www.ncsc.gov.uk/information/about-ncsc

(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;

(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 and digital forensics;

(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,	This provides the purpose and functions of the Council

efficient, effective and consultative approach in the coordination of cybersecurity initiatives, including at the counties.

(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,

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

(1) A corporate entity shall notify the National Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC) within 24 hours of any Cybersecurity incident (s) that could have a significant and adverse impact on its ability to provide adequate services to its customers, its reputation or financial condition.

(2) A notification under sub-section (1) shall include:

a) Name of the entity;
b) Date of the incident;
c) Time of incident
d) Nature of the incident
e) Effect of the incident;
f) Risk level;
g) Action taken;
h) Corrective measures taken;
i) Name of reporting officer
j) Any other relevant information.

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 an unit 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

The cybersecurity agencies shall be required to:

a) Cooperate with each other and other relevant institutions for the promotion of cybersecurity;
b) Promote multi-stakeholder approaches in their functions;

Reporting of Cyber risks

MEMORANDUM ON THE COMPUTER AND CYBERCRIMES BILL OF 2017

13TH FEBRUARY 2018

MEDIA COUNCIL OF KENYA

MEMORANDUM ON THE COMPUTER AND CYBERCRIMES BILL 2017

The following are the views of the Media Council of Kenya on the provisions of the Computer and Cybercrimes Bill 2017

COMPUTER AND CYBERCRIMES BILL 2018		
SECTION	**ISSUE OF CONCERN**	**RECCOMENDATIONS**
Section 12 False publications A person who intentionally publishes false, False publications. 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.	-This provision constitutes an unjustifiable limit on the right to freedom of expression granted under Article 33 of the Constitution. It is reminiscent of section 29 of Kenya Information and Communication (Amendment) Act 2013 on **misuse of telecommunications device** which was declared unconstitutional by the High Court. The provision fails the test set out in Article 24(2) of the Constitution with regard to legislation limiting fundamental rights and freedoms. -In a country where people are writing, tweeting, texting, or blogging every minute, it would be unreasonable to expect them to verify the truth of each statement published. -Publication of false information has been dealt with by other legislations including but not limited to the defamation Act	This section should be **deleted** in its entirety

Section 13 on Child Pornography	**-Section16 (Child Pornography) of the Sexual offences Act** has comprehensive provisions on publication of child pornography. However, the penalties for the same offences are very different from each other. -Whereas section 6 of the Sexual Offenses Act provides for a fine of not less than 500,000 and or 6 years in prison, the Bill provides for a fine not exceeding Ksh 20,000,000 and or 25 years in jail or both for more or less the same offence.	Either **delete** the entire section or in the alternative and without prejudice, the Bill should make provisions amending Section 16 of the Sexual Offenses Act that are at variance with the provisions of this Bill.
Section 16 on Cyber bullying and Cyber-stocking	Consider renaming the Section **Cyber-Harrassment** as is the best practise and is more representative of these kinds of offences. -The section does not provide for legal redress in the form of court sanctioned restraining orders	Rename the section and provide for the meaning of the word Cyber-harassment in the definition's section, Make provisions for obtaining of restraining orders for victims.

Section 17 on Aiding and abetting in the Commission of an offense	-This Section is a cut and paste of **Section 20 of the Penal Code.** Including this Section in the Bill will amount to repetition and lead to legislative confusion	This section should **be deleted**
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.	-This provision violates Article 31 on the right to privacy. It lowers the threshold for obtaining the information as provided in Sections 26(1) to (5) of the same Bill requiring a court order before execution of such production. It renders the entire section meaningless. It defeats the purpose of having a court process and provides an opportunity for abuse.	**Section 26(6)** should be deleted in its entirety

CIPIT
CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

Strathmore University
Law School

(2) EMEJOA Pls deal FA 15/2/18 (1) D[illegible] 15/2/18

TO: THE ICT COMMITTEE AND HONORABLE MEMBERS OF PARLIAMENT

FR: THE CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW, (CIPIT)

DA: FEBRUARY 13TH, 2018

RE: COMMENTS RELATING TO THE COMPUTER AND CYBERCRIMES BILL 2017

The Centre for Intellectual Property and Information Technology Law (CIPIT) would like to submit this memorandum on the Computer and Cybercrimes Bill 2017. The bill has undergone First Reading according to Parliamentary Standing Order 127 (3) and is currently committed to the Departmental Committee on Communications, Information and Innovation. The Computer and Cybercrimes Bill 2017 proposes to provide a framework to prevent and control the threat of cybercrime.

CIPIT is an evidence-based research and training centre based at Strathmore University Law School, Nairobi, Kenya. Our Mission is to study, create, and share knowledge on the development of intellectual property and information technology, especially as they contribute to African Law and Human Rights. We are based at Strathmore University Law School, Nairobi, Kenya.

Upon receipt of the call for memoranda, we called on members of the public to contribute their views on the bill which we have uploaded on the Jadili platform. Members of the public contributed their views on various issues and we have compiled them on the table below.

COMMENTS ON THE COMPUTER AND CYBERCRIME BILL 2017

Clause	*Comments*
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.	This sub-section does not protect the legitimate use of devices and programs such as 'tcpdump and wireshark' that are designed primarily to intercept and capture network traffic. They can serve a dual purpose that can be abused by malicious actors. The law should not ban them in a blanket manner but instead regulate only their malicious use.

RECEIVED 14 FEB 2018 CLERK'S OFFICE

CIPIT
Strathmore Law School
PO Box 59857-00200
Nairobi, Kenya

CIPIT@strathmore.edu
www.cipit.org

Mobile: (254-0703) 034601
Tel: (254-0705) 630310
Fax: (254-20) 6007498

PART III (Clause 22-32) Provides for investigation procedures including search and seizure of stored computer data, such power to search without warrant in special circumstances, record of and access to seized data, production order and grounds for such application of a production order by a police officer, expedited preservation and partial disclosure of traffic data, such period for preservation and extension of the said period. More procedures detailed are real time collection of traffic data, interception of content data, procedure for making application to intercept and such grounds to be satisfied before such interception. This Part also provides for confidentiality of investigations and powers to deal with obstruction of investigations.	There should be a clear explanation on qualification of who this law will regard as 'an authorised person'. We propose a qualified digital forensics expert serving in the police service.
This Bill delegates regulation-making powers to the Cabinet Secretary responsible for matters relating to Information, Communication and Technology. The Bill does not contain provisions limiting rights and fundamental freedoms.	A statement on how the legislation aligns with protections in Kenya's constitution and international obligations to protect human rights according to Article 21 of the Constitution which obligates the state to protect human rights should be front and centre of the Bill.
Statement on the delegation of legislative powers and limitation of fundamental rights and freedoms.	The Bill appears to be heavily influenced by the Council of Europe's Convention on Cybercrime (known as the Budapest Convention). But what underpins the Budapest Convention is **safeguards**, namely the UN ICCPR and the European Convention on Human Rights. A country cannot import the provisions without underpinning them with safeguards and making them meaningful. Without these safeguards, the entire Bill is extremely intrusive.
4. (1) **A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised**, commits an offence and is liable on conviction, to a fine not exceeding	This clause may criminalise security research such as penetration testing.

five million shillings or to imprisonment for a term not exceeding three years, or to both.	
10. (2) For purposes of this section— "**protected computer system**" means a computer system used directly in connection with, or necessary for, a)the security, defence or international relations of Kenya:	It is not clear whether all protected computer systems qualify as *critical infrastructure.*
11. (1) A person who unlawfully and intentionally performs or authorizes or allows another person to perform a prohibited act envisaged in this Act, in order to— a) gain access, as provided under section 4, to **critical data, a critical database or a national critical information infrastructure**; or	The bill does not define what *critical infrastructure* is.
12. 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.	This clause is unconstitutional to the extent that it limits freedom of expression beyond the limitations in Article 32 (2) of the Constitution of Kenya.
13. (1) A person who, intentionally— a) publishes **child pornography** through a computer system;	The offence already exists and can be dealt with under Section 16 (Child pornography) of the Sexual Offences Act (2006) which is quite comprehensive.
authorised person	This is not very specific as has not been clearly defined in the Bill.

28. (1) Where a **police officer** or an authorised person has reasonable grounds to believe that traffic data associated with specified communications and related to the person under investigation is required for the purposes of a specific criminal investigation, the police officer or authorised person may apply to the court for an order to—	Kenya's existing surveillance legislation only permits intelligence agencies and police officers above the rank of a Chief Inspector to apply for a warrant for this kind of surveillance (National Intelligence Services Act 2012 and the Prevention of Terrorism Act 2012). This is really expanding the scope of law enforcement's powers to undertake very intrusive surveillance, and we suggest xxxx
28. (1) a) permit the police officer or authorised person to collect or record through the application of technical means traffic data, **in real-time**	Kenya's existing surveillance framework is already very intrusive with proper safeguards or oversight. This expansion of surveillance powers in a cybercrime bill is open to abuse.
Unauthorised interception.	This is also in Section 83 of the Kenya Information and Communications Act (2009)
Record of and access to seized data.	This is similar to Section 83 of the Kenyan Information and Communication Act (2009)
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.	It is not clear what these "special circumstances" are exactly. The law should include examples of these special circumstances for example in situations of organised crime like terrorism and drug trafficking.

28. Real-time collection of traffic data.	As outlined below, this is a massive expansion of Kenya's surveillance powers, which is already intrusive and without safeguards, accountability or transparency.
29. Interception of content data.	This is a massive expansion of the Government of Kenya's surveillance powers, which is already intrusive and without safeguards, accountability or transparency. A warrant should be sought before commencement of the interception.
24. Power to search without a warrant in special circumstances.	This should be removed as it can be used to infringe on human rights such as the right to privacy.
(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 section. Let the Judiciary have oversight for this as rightly mandated by the constitution.
34. (1) The Central Authority may, subject to this Act and any other relevant law, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings concerning criminal offences or might lead to a request for co-operation by the foreign State under this Act.	Judicial oversight also needed in this clause

CIPIT
Strathmore Law School
PO Box 59857-00200
Nairobi, Kenya

CIPIT@strathmore.edu
www.cipit.org

Mobile: (254-0703) 034601
Tel: (254-0705) 630310
Fax: (254-20) 6007498

25

COMMUNICATIONS AUTHORITY OF KENYA

Our Ref: CA/LS/NA/050/18(128)

19th February, 2018

Michael R. Sialai, EBS
Clerk of the National Assembly
Clerk's Chambers
National Assembly
Parliament Buildings
P.O. Box 41842 - 00100
NAIROBI

RECEIVED
21 FEB 2018
CLERK'S OFFICE

Dear Sir,

RE: SUBMISSION OF MEMORANDA ON COMPUTER AND CYBERCRIMES BILL 2017

We refer to the above matter.

We are in receipt of the invitation through a Public Notice (as attached) to participate in submitting comments on the Computer and Cybercrimes Bill 2017.

In this regard, we find that the Computer and Cybercrime Bill, 2017 provides for a framework for timely and effective detection, investigation and prosecution of computer related and cybercrime offences as well as the critical element of international co-operation in dealing with computer and cybercrime incidences.

We herewith attach a copy of our Memorandum (Proposals) on the Bill and look forward to having audience with the legislators so as to clarify any issues that may not be clear.

Yours faithfully

Christopher K. Kemei
FOR: DIRECTOR-GENERAL

CA Centre, Waiyaki Way |P.O. Box 14448, Nairobi, 00800, Kenya|T: +254 (20) 4242000
M: 0703 042 000, 0730 172 000 Fax :+254 (20) 4451866|www.ca.go.ke|E: info@ca.go.ke

who are in school and who depend on her for food and fees.

The children ... mostly ... from diverse backgrounds. (Gardy Chacha, Sta...

REPUBLIC OF KENYA

NATIONAL ASSEMBLY
TWELFTH PARLIAMENT – FIRST SESSION

In the Matter of consideration by the National Assembly - The Computer and Cybercrimes Bill, 2017

SUBMISSION OF MEMORANDA

Article 118(1) (b) of the Constitution provides that, *"Parliament shall facilitate public participation and involvement in the legislative and other business of Parliament and its Committees".*

Further, Standing Order 127(3) provides that, *"the Departmental Committee to which a Bill is committed shall facilitate public participation and shall take into account views and recommendations of the public when the Committee makes its report to the House".*

The Computer and Cybercrimes Bill, 2017 proposes to provide a framework to prevent and control the threat of cybercrime, that is, offences against computer systems and offences committed by means of computer systems.
The Computer and Cybercrimes Bill, 2017, has undergone First Reading pursuant to Standing Order 127(3) and is now committed to the **Departmental Committee on Communications, Information and Innovation** for consideration and thereafter report to the House.

Pursuant to Article 118(1)(b) and Standing Order 127(3), the Committee invites members of the Public to submit any representations they may have on the Computer and Cybercrimes Bill, 2017. The representations may be forwarded to the **Clerk of the National Assembly, P.O. Box 41842-00100, Nairobi;** hand-delivered to the **Office of the Clerk, Main Parliament Buildings, Nairobi;** or emailed to **clerk@parliament.go.ke;** to be received on or before **Tuesday 13th February, 2018 at 5:00 pm.**

MR. MICHAEL R. SIALAI, EBS
CLERK OF THE NATIONAL ASSEMBLY

COMMUNICATIONS AUTHORITY OF KENYA

PROPOSALS FOR THE COMPUTER AND CYBERCRIMES BILL, 2017

No	Current text	Proposal/Comments	Justification
		PART I – PRELIMINARY	
1.	New Proposal	In the preliminary section the Bill makes reference to the Mutual Legal Assistance Act and no mention of the Extradition (Contiguous & Foreign Countries) Act	Both the Mutual Legal Assistance Act and the Extradition (Contiguous & Foreign Countries) Act are complementary in ensuring the successful prosecution of offences under this proposed law.
		PART III- INVESTIGATION PROCEDURES	
2.	Section 24(1) Power to search without a warrant	(a) Define a criteria for situations that would meet the threshold for 'special circumstances	a. Waiver for the requirement for a warrant in advance of undertaking a

	in special circumstances		search has the huge potential of infringing on constitutional rights an liberties, hence the need to be achieve with clarity circumstances under which this requirement would be waived in order to provide a an objective framework within which to evaluate applications. b. S. 24(2) – Section 119, 120 and 121 of the Criminal Procedure Code cited to serve as guidance are very removed from the reality of the speed and sophistication attendant to cybercrime and may need to be infused with this reality.
PART IV-INTERNATIONAL COOPERATION			
3.	Section 41 Point of Contact	Delete 'and prosecuting cybercrime' from the third line as it creates a conflict of interest.	The point of contact should be the investigating agency only in order to

			promote independence of roles.
4.	General Comment		The success of implementation of this draft law will rest on a number of institutions, among them the NPS, NIS, CA, KDF, ODPP etc. If there is need to formalize collaboration, an appropriate home within an agency empowered to handle the key elements of this law including the mutual legal assistance aspect would be the ideal host.

66

KEPSA
KENYA PRIVATE SECTOR ALLIANCE

The Voice of Private Sector in Kenya

(1) D/Cmttee 15/2/18

RECEIVED
14 FEB 2018
CLERK'S OFFICE

(2) Engage pls deal FA 15/2/18

Ref: 14/02-PPD/2018

February 14, 2018

Mr. Michael Sialai , EBS
The Clerk
The National Assembly,
Parliament Buildings
Nairobi.

Dear Mr. Sialai,

RE: KEPSA SUBMISSION ON THE COMPUTER AND CYBER CRIMES BILL, 2017

Receive greetings from the Kenya Private Sector Alliance (KEPSA).

Following your request for public input into the Computer and Cyber Crimes Bill, 2017, KEPSA is pleased to submit to your office the Submission Memoranda of suggested amendments on behalf of its members.

Further, KEPSA ICT Sector Board will be available to appear before the Departmental Committee on ICT to defend the input or clarify any issue that may arise from our submission.

We wish to register our appreciation for the invitation to submit comments and look forward to continued engagement and co-operation with the National Assembly on legislative matters.

Yours Sincerely,

Carole Kariuki, MBS, HSC
Chief Executive Officer

Encl:
KEPSA Submission

5th Floor, Shelter Afrique Building, Mamlaka Road | P. O. Box 3556 - 00100, Nairobi, Kenya | Tel: +254 20 2730371|2|2727936 | Fax: +254 20 2730374
Cell: +254 720 340949/735 999979 | Email: info@kepsa.or.ke | Web: www.kepsa.or.ke

MEMORANDUM BY KENYA PRIVATE SECTOR ALLIANCE, (KEPSA) ON THE COMPUTER & CYBERCRIMES BILL, 2017

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
Part 1-Preliminary		
At Clause 2 "computer system" means a physical or virtual device, or a set of associated physical or virtual devices, which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and communication functions on data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer system includes a reference to part of a computer system; 'interception" means the	**Include definition of:** include 'automatic processing of data' as part of computer system Definition of the "interception" should be aligned more closely	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, and may help ensure inclusion of "Internet of Things" devices The definition of 'interception' –

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
monitoring, modifying, viewing or recording of non- public transmissions of data to or from a computer system over a telecommunications system, and includes, in relation to a Function of a computer system, listening to or recording a function of a computer system or acquiring the substance, its meaning or purport of such function; **New Definition**	with the definition of "illegal interception", as put forward in Article 3 of the Budapest Convention on Cybercrime. **Critical Information Infrastructure** refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to the Republic of Kenya that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.	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. The meaning of critical information infrastructure is not clear/defined in Part II-Offences, Clause 11 (1) (a) on Cyber Espionage
Clause 18 (1) (b) 18. (1) (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	**Reword Clause 18 (1) (b)** 18. (1) (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, **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, is also deemed to have committed the offence and liable**, on conviction, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years,	**Rewording Clause 18 (1) (b) meets the Constitutional requirement of Fair Hearing at Article 50 Clause 2 (a)** **Fair hearing.** **50.** (1) Every person has the right to have any dispute that can be resolved by the application of law decided in a fair and public hearing before a court or, if appropriate, another

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
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, to a fine not exceeding five million shillings or imprisonment for a term not exceeding three years, or to both.	or to both.	independent and impartial tribunal or body. (2) Every accused person has the right to a fair trial, which includes the right— (*a*) to be presumed innocent until the contrary is proved;
Clause 22 (3) The powers and procedures provided under this Part are without prejudice to the powers granted under— the National Intelligence Service Act, 2012; the National Police Service Act, 2011; the Kenya Defence Forces Act, 2012; and any other relevant law.	**Delete this section.** The powers and procedures provided under this Part are without prejudice to the powers granted under the National Police Service Act, 2011 and any other relevant law.	This will be giving a blanket approval for the officers for the NIS and KDF who are not envisaged to be the authorized personnel. The officer of this institutions would normally not be going to apply for the court orders that must be obtained, hence may not be in compliance with the requirement of this act in their operations. "authorized person" means a person designated by the Cabinet Secretary by notice in the Gazette for the purposes of Part III of this Act;

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
23(1): Where a police officer or an authorized person has reasonable grounds to believe that there may be in a specified computer system or part of it, computer data storage medium, program, data that- (a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence; or (b) has been acquired by a person as a result of the commission of an offence, the police officer or the authorized person **MAY** apply to the court for issue of a warrant to enter any premises to access, search and similarly seize such data.	23(1): Where a police officer or an authorized person has reasonable grounds to believe that there may be in a specified computer system or part of it, computer data storage medium, program, data that- (c) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence; or (d) has been acquired by a person as a result of the commission of an offence, the police officer or the authorized person **SHALL** apply to the court for issue of a warrant to enter any premises to access, search and similarly seize such data.	The use of the word 'may' gives a discretion to a police officer to decide whether he should or should not obtain a court order before entering, searching and seizing property. The Constitution of Kenya, section 31 establishes the right to privacy as the right of a person not to have their person, home or property searched. Article 24(3) of the Constitution states that "The State or a person seeking to justify a particular limitation [of a right and fundamental freedom] **shall demonstrate to the court**, tribunal or other authority that the requirements of this Article
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	Delete the entire section, or, outline the special circumstances where warrant shall not required	While the previous section provides for search by warrant (albeit discretionally), this section effectively does away with a search warrant in 'special circumstances' without defining what those special circumstances are; or;

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
computer system		To provide clarity on what special circumstances would exist to allow a police officer enter a suspected premise without a warrant.
26. (1). Where a police officer or an authorized person has reasonable grounds to believe that ...subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control and is necessary or desirable for the purposes of the investigation, the police officer or the authorized person **MAY** apply to court for an order requiring [the production of the information]	26. (1). Where a police officer or an authorized person has reasonable grounds to believe that ...subscriber information relating to services offered by a service provider in Kenya are in that service provider's possession or control and is necessary or desirable for the purposes of the investigation, the police officer or the authorized person **SHALL** apply to court for an order requiring [the production of the information]	The use of the word 'may' gives a discretion to a police officer/ authorized person to decide whether he should or should not obtain a court order before entering, searching and seizing property.
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	**Delete the entire section**	While the previous section provides for search by warrant (albeit discretionally), this section effectively does away with a search warrant again at the discretion of the police. Under the provisions of the Constitution set out above, it would be unconstitutional to restrict the right to privacy

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
provider's possession or control which is necessary or desirable for the purposes of any investigation, the designated Officer may order such a provider to submit subscriber information relating to such services in that service provider's possession or control.		outside of the framework set out in those articles on how a law limiting such a right should be crafted and the court process.
Section 28(1): Where a police officer or an authorized person has reasonable grounds to believe that traffic data associated with specified communications and related to the person under investigation is required for the purposes of a criminal investigation, the police officer or authorized person **MAY** apply to the court for an order to [collect and/or compel a service provider to collect and disclose real time data	Section 28(1): Where a police officer or an authorized person has reasonable grounds to believe that traffic data associated with specified communications and related to the person under investigation is required for the purposes of a criminal investigation, the police officer or authorized person **SHALL** apply to the court for an order to [collect and/or compel a service provider to collect and disclose	The use of the word 'may' gives a discretion to a police officer/ authorized person to decide whether he should or should not obtain a court order in order to collect or compel a service provider to disclose real time traffic data
29. (1) Where a police officer or an authorized person has reasonable grounds to believe that the content of any specifically identified electronic communications is required for purposes of a specific investigation in respect of a	29. (1) Where a police officer or an authorized person has reasonable grounds to believe that the content of any specifically identified electronic communications is required for purposes of a specific investigation in respect of a serious offence, the police officer or authorized person **SHALL** apply to the court for an order to- [collect or compel a service provider to collect and disclose] content data, in real-time, of specified communications....transmitted by means of a computer system.	The use of the word 'may' gives a discretion to a police officer/ authorized person to decide whether he should or should not obtain a court order in order to collect or compel a service provider to disclose real time traffic data transmitted by means

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
serious offence, the police officer or authorized person **MAY** apply to the court for an order to- [collect or compel a service provider to collect and disclose] content data, in real-time, of specified communications....transmitted by means of a computer system.		of a computer system
32. (1) A service provider shall not be subject to any civil or criminal liability, unless it is established that the service provider had actual notice, actual knowledge, or willful and malicious intent, and not merely through omission or failure to act, had thereby facilitated, aided or abetted the use by any person of any computer system controlled or managed by a service provider in connection with a contravention of this Act or any other written law.	**Delete the current provisions of section 32 and replace them with the following provisions:** 32 (1) There is no obligation on the part of a service provider involved in the facilitation of the dissemination of information to proactively monitor that information, or make inquiries about content hosted, cached, routed, transmitted, or otherwise processed in the course of providing services. (2) A service provider has no liability for damages or other monetary relief to any person in respect of content complained of, if, upon receiving a valid notice, the online service provider acts expeditiously to remove or block access to the content. (3) A notice from a complainant is only valid if it meets the following conditions. (a) a court has adjudicated that the complainant has legal standing to assert a claim (or is an agent acting on behalf of such	Internet intermediaries is a broad term which includes different kinds of business models critical to both the internet and the small and medium business ecosystem - website hosting companies, internet service providers (ISPs), information search and retrieval service providers, social media platforms - who play a crucial role in enabling people to access the internet and in transmitting third-party content. Internet intermediaries are distinct from 'content producers', who are responsible for producing information in the first place and posting it online. Intermediaries simply provide the infrastructure for the sharing of

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
	a complainant) and that the content is clearly and unambiguously unlawful (b) provides physical or electronic signature of a person authorized to act on their behalf (c) sets out the specific content to be removed, clearly identifying it by its online address where available, or other unique identifier where not; (d) attests to the good faith and validity of the claim and obtains a court order determining that the content is illegal. (e) includes information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and an electronic mail address at which the complaining party may be contacted. (f) 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. (4) If a service provider receives a valid counter-notification, then they cannot be held liable for damages or other monetary relief for the content. (5) A counter notification is only valid if it meets the following conditions. (a) the entity or person submitting the counter-notification was	content and have nothing to do with the content itself. Throughout the world, including in the African Union, the general principle that intermediaries should not be liable for their user's content, and that therefore they should not have any general legal obligation to monitor user content or be responsible for its accuracy, its maintenance and it's annotating, has been recognized This principle has its strongest foundations in freedom of expression and individual privacy, which are rights guaranteed both by the Constitution of Kenya as well as regional and international law. In order to serve this broad purpose, the proposed amendment is in line with international best practices on the ideal law on intermediary liability protection, which meets the following criteria:

Current Clause in the Bill	Proposed Amendment	Rationale and Justification
	accused of violating the law, responsible for making available the specific content that was removed. (b) provides physical or electronic signature of the person or entity, or a third-party authorized to act on their behalf (c) attests to the good faith and validity of the claim that the content is lawful; (d) includes information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and an electronic mail address at which the complaining party may be contacted. (6) Any person who knowingly materially misrepresents under this section— (a) that material or activity is unlawful, or (b) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including punitive damages, costs and fees, incurred as a result. (7) A 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 material, regardless of whether the material or activity is ultimately determined to be legal or illegal.	a) Removal obligations should pertain to illegal content b) Intermediaries should have no general monitoring or filtering obligation for illegal content; c) Instead, any removal requirements should be part of a well-balanced notice and takedown system; and d) Fair process and protections against abusive removals - including meaningful requirements for what constitutes a valid removal request (e.g., clearly identifying the content at issue by URL; a clear statement of the basis of the legal claim); a robust ability for both users and service providers to contest such requests.

67

ICTAK

Information Communication Technology Association of Kenya

IMPROVING LIVES THROUGH ICT

P.O. Box 17429-00100 Nairobi;, PSC Wing, 9th Floor, Hazina Towers: Mob: 0731 786 644;

E-Mail: secretarygeneral@ictak.or.ke; www.ictak.or.ke

13th February 2018

Mr. Michaael R. Sialai, EBS,
Clerk of the National Assembly,
Republic of Kenya,
Main Parliament Buildings,
P.O. Box 41842-00100,
Nairobi.

DS/Committees.
14/2/18

Dear Sir,

MEMORANDUM ON THE COMPUTER AND CYBERCRIMES BILL 2017

(KNA/DCS-CII/2018/003)

Receive warmest compliments from the ICT Association of Kenya. In response to your letter dated 6th February 2018 requesting for memoranda on the above Bill, may it please you to consider the annexed memorandum which summarizes our views with regard to the Bill.

We look forward to further engagement on the subject matter of the Bill.

Sincerely,

(2) Enough
pls deal
15/2/18

Kamotho Njenga

Secretary General
ICT Association of Kenya

Information Communication Technology Association of Kenya
ICTAK
IMPROVING LIVES THROUGH ICT
P.O. Box 17429-00100 Nairobi;, PSC Wing, 9th Floor, Hazina Towers: 0731 786 644; secretarygeneral@ictak.or.ke; www.ictak.or.ke

PROPOSALS FOR REVIEW: THE COMPUTER AND CYBERCRIMES BILL 2017

CLAUSE	PROVISION	COMMENT/PROPOSAL	RATIONALE
Title	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 for assurance of computer and cyber security; prevention, investigation and prosecution of cybercrime; management of cybersecurity affairs; and for connected purposes.	To holistically capture all the cyber security areas of concern
2	Interpretation	Insert the following definition "Cybersecurity" means the entire collectivity of technologies, processes, procedures, methods and practices designed to protect systems, devices, networks, computers, programs and data from attack, impairment, damage, destruction, obliteration, degradation or unauthorized access. "Authority" means the National Cyber Security Authority established under this Act	Definition is necessary for clarity
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 is ambiguous and may be abused. May fetter free flow of information in a digital age

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	Clause infringes on Article 31 of the Constitution

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	A court process should be involved to avert possible abuse of this provision

New Provisions to anchor the Proposed National Cyber Security Authority	Establishment of Cybersecurity Authority of Kenya (1) There is established a body to be known as the National Cybersecurity Authority of Kenya (2) The Authority shall be a body corporate with perpetual succession and a common seal and shall, in its corporate name, be capable of—- (a) suing and being sued; (b) taking, purchasing or otherwise acquiring, holding, charging and disposing of movable and immovable property; (c) borrowing or lending money; and (d) doing or performing all such other things or acts for the proper performance of its functions under this Act which may be lawfully done or performed by a body corporate. (3). The Headquarters of the Authority shall be in Nairobi.	A National Cyber security Authority is extremely necessary towards the coordinated administration, management and governance of Cybersecurity matters in Kenya

Object and Powers of the Authority

(1) The object and purpose for which the Authority is established shall be provide centralized oversight of national cyber security in accordance with the provisions of this Act.

(2) The Authority shall have all powers necessary for the performance of its functions under this Act.

(3) The Authority may enter into association with such other bodies or organizations within or outside Kenya as the Authority may consider desirable or appropriate and in furtherance of the purpose for which the Authority is established.

(4) The Authority shall, in the performance of its functions under this Act have regard to—

(a) any policy guidelines of a general nature relating to the provisions of this Act notified to it by the Minister and published in the Gazette;

(b) Kenya's obligations under any international treaty or agreement relating to cybersecurity.

Board of the Authority

(1) The management of the Authority shall vest on the Board which shall consist of—

(a) a chairperson appointed by the President;

(b) the Principal Secretary for the time being responsible for matters relating to Information Communication and Technology or his or her representative;

(c) the Principal Secretary for the time being responsible for matters relating to finance or his or her representative;

(d) the Principal Secretary for the time being responsible for matters relating to internal security or his or her representative; and

(e) Three persons not being public officers with demonstrated experience of not less than five years in the information, communication and technology sector appointed by the Cabinet Secretary;

f) The Attorney General or his or her representative

g) the Director of Public Prosecutions

h) the Director-General of the Communications Authority, or his or her representative

i) the Inspector-General of the National Police or his or her representative

j) The Chief Executive Officer who shall be an Ex-officio member and the Secretary to the Board

Functions of the Cybersecurity Authority

a) Formulate relevant policies with regard to cybersecurity;

b) Continuously develop and implement strategies to improve cybersecurity in Kenya;

c) Assist all government entities in cybersecurity assurance;

d) Collate data relating to cyber security incidents across the country

e) Provide regular reviews recommendations on ways of enhancing cyber security.

f) Engage with stakeholders to create a resilient and trusted cyber environment

g) Coordinate cyber security incident response missions

h) Conduct research, and disseminate information on cyber security;

i) Create awareness and preparedness on cybersecurity and

j) Perform other tasks as may be necessary under this Act

The Chief Executive Officer

(1) The Chief Executive Officer shall be the chief executive officer of the Authority and shall be responsible for the day to the day management of the Authority.

(2)
The Chief Executive Officer shall be an ex officio member of the Board but shall have no right to vote at any meeting of the Board.

(3) The Chief Executive Officer shall be appointed by the Cabinet Secretary on the recommendations of the Board.

(4) The Board shall determine the terms and conditions of service of the Chief Executive Officer, in consultation with the Public Service Commission.

(6) The Chief Executive Officer shall be appointed for a term of three years renewable once.

Zimbra clerk@parliament.go.ke

Computer and Cyber Crime Bill 2017

From : David Ogiga <david@sotehub.com> Thu, Feb 08, 2018 05:46 PM
Subject : Computer and Cyber Crime Bill 2017 1 attachment
To : clerk@parliament.go.ke
Cc : collins oduor <collins.oduor2012@gmail.com>

Dear Mr. Michael Sialai, MBS,

I trust this email finds you well.

We would like to propose **Mr. Collins Oduor** to represent Sote Hub in **Computer and Cyber Crime Bill 2017.**

Please find enclosed the official letter.

We look forward to your kind feedback.

Warm Regards,
David

Collins Oduor Letter.jpeg
2 MB

February 08, 2018

Mr. Michael Sialai, MBS,
Clerk of the National Assembly
P.O Box 41842-00100
Parliament Buildings
Nairobi

Dear Sir,

RE: COMPUTER AND CYBERCRIME BILL 2017

Receive warm greetings from Sote Hub community in Voi and Kwale

We would like to appoint**Mr. Collins Oduor ID No. 25279129** to represent Sote Hub in the**Computer and Cybercrime Bill 2017.**

We look forward to your kind feedback.

Sincerely,

Sote ICT
Information, Communication &Technology
P. O. Box 900-80300, VOI
www.sotehub.com

David Otieno Ogiga
Executive Director

SUBMISSION OF MEMORANDA

Computer and Cybercrimes bill 2017.

Missing on offences;

1. Anyone who sets up a website or publishes information for a terrorist group or criminal group or gang under fake names with intent to facilitate contacts with their leadership or to promote their ideology and finance their activities or publish information on how to make explosives or any other substances to be used in terrorist attack is an offence.
2. Anyone who logs onto a Govt website with intent to obtain secret information is an offence. If this results to destruction, deleting or publishing such information is a crime.
3. Anyone who transfers dirty money or concealing their sources or transfers illegal properties via the use of internet or through other high tech means is an offence
4. Anyone who assists or agrees with other person(s) to commit a crime or crimes stipulated in this law, shall be punished with the same punishment stipulated in the law.
5. All devices, programs and means used in committing any mentioned crime will be confiscated.
6. If a convict to this crimes is an expatriate, he or she shall be deported after serving his term.
7. Implementation of penalties stipulated in this law does not contradict any other tougher punishment stipulated in the penal code or any other laws.
8. Anyone who intentionally destroys or reveals secrets or republishes official information through the internet or through other high tech means is a crime.
9. Anyone who intentionally destroys or reveals secrets or republishes official information is a crime.
10. Anyone who abuses, insults or opposes a recognized religion is an offence
11. Anyone who forges Govt documents, either National or county Govt is an offence
12. Anyone who inserts certain information via the internet or uses any IT or electronic means for the purpose of destroying, deleting or amending a program or information commits an offence.
13. Deliberate eavesdropping, intervened information or messages sent via the internet by use of electronic or high tech means is an offence.

14. Any person who uses the internet or any other high tech means to threaten, blackmail another person, to incite him carryout an act or not is an offence.
15. Any person who uses the internet or any other high tech means in a fraudulent way by assuming the identity of others with intent to defraud is an offence.
16. Anyone who reaches data, mobile money transaction data, credit card or any other electronic cards by the use of internet or through any other high tech means is an offence.
17. Anyone who reaches information or data to produce, save, prepare, send information with intent to exploit, distribute or provide to others that information that causes harm to public decency via the internet or through high tech means is a crime.
18. Anyone who lures male or female to commit adultery or prostitution by using the internet or through other high tech means is an offence.
19. Anyone who logs into a website with intent to change the designs of the site, deleting it, amending its information or taking its address or bring it down, intentionally jams the network is an offence.
20. Anyone who publishes transcending private life of a family, including news, pictures all related to private life of the family is an offence.
21. Anyone who sets up a website or publishes information with the aim of publishing narcotics and other banned substances is an offence.

Technology Service Providers Association of Kenya,
Bruce House-Standard Street | 14th Floor,
P.O Box 27589-00506 Nairobi,Kenya.
info@tespok.co.ke | Tel: +254-20-2245 036
www.tespok.co.ke

OUR REF:TESPOK006/02
YOUR REF: KNA/DCS-CII/2018/003

13th February 2018

MR. MICHAEL R. SIALAI, EBS
CLERK OF THE NATIONAL ASSEMBLY
CLERKS CHAMBERS
NATIONAL ASSEMBLY
PARLIAMENT ROAD
NAIROBI

Dear Mr. Sialai

REF: SUBMISSION ON COMPUTER AND CYBERCRIME BILL 2017

We accept receipt of you letter dated 6th February 2018 Ref: KNA/DCS-CII/2018/003 where you invited the Technology Service Providers of Kenya to submit their views on the Computer and Cybercrime Bill 2017.

We hereby, attached a copy of our memorandum on the bill and look forward to having audience with the legislators so as to clarify any issues that may not be clear.

We look forward to your support.

Yours Sincerely ,

FIONA ASONGA
CHIEF EXECUTIVE OFFICER

RECEIVED
13 FEB 2018
CLERK'S OFFICE

CONSOLIDATED MEMORANDUM INCORPORATING THE SPECIFIC POSITIONS AND RECOMMENDATIONS OF TECHNOLOGY SERVICE PROVIDERS ASSOCIATION OF KENYA (TESPOK) ON THE PROPOSED AMMENDMENTS ON THE COMPUTER AND CYBER CRIMES BILL 2017

A. Introduction

Technology Service Providers Association of Kenya (TESPOK) has observed several attempts to develop cyber security laws over the years. The ICT Ministry together with the Kenya Law Reform Commission (KLRC) led in the drafting of the *Computer and Cyber Crimes bill of 2016*. The Bill was on 6th April 2017 approved by Cabinet and forwarded to the Attorney General for publication before tabling in the National Assembly.

The objective of the Computer and Cyber Crimes Bill is to provide for offences relating to computer systems; such timely and effective collection of forensic material for use as evidence, and facilitate international co-operation in dealing with cybercrime matters. Although TESPOK was involved in the development of the Bill, some critical industry proposals and positions were ignored by the drafters who lacked sufficient appreciation of the business environment, how the industry operates and global industry standards of practice. Some of the key provisions contained in the current Bill which could have adverse negative effects in the sector if allowed to remain as currently stated include:

B. Analysis of the Legislative Proposal

	CLAUSE	TITLE AND PROVISION	TESPOK COMMENTS	TESPOK PROPOSED AMMENDMENT	JUSTIFICATION
1.	Clause 8	This clause outlines penalty for the offence of illegal device.	The term illegal device has not been defined.	It is proposed that the word illegal device be included in the definition section	To ensure that there is clarity on what an illegal device is and when a device can be declared illegal
2.	Clause 13	The clause provides for the offence of child pornography.	The definition of publish includes transmit that are key functions of internet service providers of content from different sources.	It is our proposal that transmission being a core function of ISPs be excluded from the meaning of publish as stated in the bill.	Intermediaries will be held responsible for data transmitted through their infrastructure, while the content developers may end up getting away. This is costly and impractical with the service providers and places onerous financial and technical burdens on service providers.

3.	Clause 23	The clause provides for search and seizure of stored computer data	The requirement to define an authorised person Definition of stored data that an investigation officer seize a computer system during an investigation is impractical as it will have heavy implications on the business environment.	It is the Industry's proposal that; *the authorised person be a police officer specifically designated to handle cyber security* *Stored data is information that can be retrieved at a later time from an existing computer device or system*	This provides clarity on who ia authorised to search premises and reduces abuse
4.	Clause 24	The power to search without a warrant in special circumstances	The wording special circumstances does not make it concise as to when there would be a search without a warrant. The clause ignores the	It is proposed that these circumstances be specifically defined or the clause be deleted	This will provide clarity on what the special circumstances are that will allow for a search without a warrant.

			technical concept of remote access.		
5.	Clause 28	The clause provides for expedited preservation and partial disclosure of traffic data.	Data moves very fast over networks through switches don't store data. Traffic data is not static making it difficult to collect.	The proposal requires specific definition of the word *'stored data'* to avoid confusion.. *Stored data is information that can be retrieved at a later time from an existing computer device or system*	This provides clarity and reduces abuse
6.	Clause 29	The clause provides for interception of content data	This gives lee way for breach of privacy rights	It is proposed that this clause be deleted. The provisions be included in the data protection laws.	May expose service providers to litigious matters.

(2) Emeru
pls deal
FA
14/2/18

Michael Otieno Odhiambo
P.O Box 40241-00100
modhiambo@kws.go.ke
C/O Kenya Wildlife Service
NAIROBI

12th February, 2018

(1) DD/Committees
13/2/18

The Clerk of the National Assembly.
P.O Box 41842-00100,
NAIROBI.

Dear Sir,

RE: COMPUTER AND CYBER CRIME BILL 2017 REPRESENTATION

Reference is made to your public notification on print media regarding submission of memoranda for the Computer and Cybercrimes Bill 2017.

Pursuant to the article 118 (1)(b) and standing order 127 (3), I would like to make my representation on the Computer and Cybercrime Bill, 2017 as a citizen of Kenya with the comments below;

1. It is worth noting that the Computer and Cybercrime Bill, 2017 as written seems to have the assumption that the bill is geared towards Government installations where there is an entity being the subject of investigation, this comment is based on the fact that clause No 2 on Pg 697 defines authorized persons as one who has been designated by the cabinet secretary by gazette notice. This may be a challenge to enforce in cases where a private investigation is constituted within a private firm where a private investigator is hired. This may also be a challenge to enforce in cases where a private corporate firm is being investigated by foreign investigating bodies that are not necessarily Government based, hence the authorized person in this case, may indeed be duly authorized by the private firm in Kenya, but not recognized by the cabinet secretary's gazette notice. My recommendation to define the scope in which the cabinet secretary's gazette notice would have an authorized person, eg in the case of Kenya Government based Ministries, Parastatals, etc.

2. Clause 23(b) states the need for a warrant from a court of law to access data for investigation purposes. I would propose that the investigating officer or the authorized person to ensure the following despite having a warrant so as to safeguard the integrity of the data or the operations of the application or program making sure it is not affected by the actions of the investigating officer or entity.
    a. Access to the data or application program is only done in the presence of the premises employee of the entity that is responsible for the data, this is done in practice but needs to be highlighted in the proposed bill.
    b. and, access to the data or application program is done with the knowledge of an employee of the entity that is responsible for the data and must be done in writing.

3. In addition to the clause 23(b) above, it should be the responsibility of the investigating authority to ensure confidentiality of the data accessed from the premises of interest. This is to critical so as to safeguard that the investigating authority does not share the data or carelessly store the data in a state that can easily be accessed by other third parties and thus compromise the information that may be customer related data consisting of contacts, purchase transactions etc. This is also to ensure that the bill is not in contradiction with the pending Data Protection Bill of 2013 when it comes to law.

4. Clause 23(4) where a police officer or the investigating authority needs to extend their search to other systems. I would propose in this case the need for the officer to officially notify the Data or application program owner of the intended extension of their search and seek authority for the same, where this is declined, a court order or warrant may be pursued by the investigating officer. This is critical to ensure data privacy on behalf of clients given that data held with customer information is the responsibility of the data holding organization or entity and they take full responsibility of any downtime of such services or breach of data, or effect of any change on the data in the cause of accessing the same for purposes of an investigation as such ensuring the Bill of rights as enshrined on our constitution of Kenya.

5. Clause 23(5) mentions data to be used for what it is meant for. I would propose for this clause to state the consequences of the data being used for other purposes other the intended reason for obtaining it, it needs to state the applicable fine an or penalty within the clause as mentioned for ease clarity so as to ensure that the bill is not seen

to be biased towards the general investigating authority with no repercussion for wrong doing of its officers. There needs to be a deterrent given that customer data is the responsibility of the source of the data and if mis-handled or shared without consent, the data owner or source is usually held liable for the same as they have an engagement with clientele and not the investigating officer.

6. Clause 24(1) is bound to be very controversial, there is major concern in allowing ad-hoc search be done in the absence of a warrant, this is in contradiction of Chapter 4 of the Constitution of Kenya, under the Bill of rights, article 31 that states "every person has the right to privacy, which includes the right not to have:
   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. privacy of their communications infringed."

   It is my considered view that this part of the bill be deleted so as to ensure the Bill has high chances of acceptance by the general public as well as make it feasible to implement and acceptance of the same. If implemented with this clause as is, it would be in contradiction of the article 31 of the constitution of Kenya.

7. Failure to consider proposal No 6 above to ensure acquisition of a warrant before accessing a premises/ computer, would lead to a high likelihood of litigation based on article 22(1) under Chapter 4- Bill of rights being invoked by a citizen, the article states "every person has the right to institute court proceedings claiming that a right or fundamental freedom in the bill of rights has been denied, violated or infringed, or is threatened."

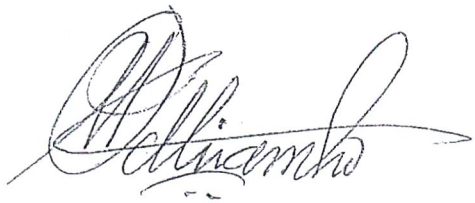
8. Clause 24(2) makes reference to the criminal procedure code sections 119, 120 and 121. It should be noted that these clauses refer to a situation where a warrant has been accessed or is to be accessed;
   a. Chapter 75 of the criminal code procedure section 119 requires that a search warrant be obtained between sunrise and sunset including Sunday and does not mention any access in the absence of a search warrant.
   b. Section 120(1) of the criminal code procedure makes reference of access for a person who already has a warrant upon which free access can be allowed.

c. Section 120(2) of the same criminal code procedure makes reference of the option available to the officer who is in possession of a warrant.

Implementing clause 24 may be in contradiction to the criminal code procedure chapter 75 as well as Chapter 4 of the Bill of rights article 31 of the constitution of Kenya that defines the right to privacy.

9. Clause 38 may be a challenge to implement given that the data privacy laws of most foreign countries where data is resident for cloud hosted solution may require explicit authorization for its access, it may therefore no be feasible to expect access without authorization on this clause and the same should be considered for amendment. Jurisdiction of data laws is dependent on the hosting country in most cases and hence this may be difficult to uphold.

It is my prayer that my concerns above are considered as part of the necessary amendments in the Computer and Cybercrime draft Bill, 2017 with a view to enrich the document and ensure acceptance of the same within the ICT industry in the country at large.



MICHAEL OTIENO ODHIAMBO

(2) EMEGER
Pls deal
FA 14/2

(1) D/Cmttee
13/2/18

(2)

ARTICLE 19

ARTICLE 19 EASTERN AFRICA

ORGANIZATIONAL BACKGROUND.- ARTICLE 19 Eastern Africa is a regional human rights organisation duly registered in 2007 as a non-governmental organisation in Kenya. It operates in 14 Eastern Africa countries and is affiliated to ARTICLE 19, a 30 year old leading international NGO that advocates for freedom of expression collaboratively with over 90 partners worldwide. We lead advocacy processes on the continent on behalf of and with our sister organisations ARTICLE 19 West Africa and ARTICLE 19 Middle East and North Africa.

Over the past 10 years, we have built a wealth of experience defending and promoting digital rights at the local, regional, and international levels. We have contributed to several Internet Freedom Policies, Data Protection and Cybercrime Bills including the Draft Uganda Data Protection Bill, the Kenya Cybercrime and Computer Related Crimes Bill 2014 and the Tanzania Cybercrime Act, 2015 among many others. We were also part of the Inter-Agency Technical Committee of the Ministry of ICT that developed the Kenya Cybercrime Bill, 2016.

Clause	Provision	Proposal	Justification
Section 3	Objects of the Act	Please insert the following "to protect human rights online as offline"	This will take into consideration best practices in developing cyber laws and the UN resolution
Section 4 of the Act	unauthorised access	Please insert the words 'with intent to defraud' to be added as a yardstick for determining whether this offence has been committed.	The clause as it is provides a very low threshold of intent which is open to abuse.
Section 5	Unauthorised access with intent to commit a further offence	Please delete clause	the reference to offences under "any other law" is too broad.
Section 6	Intentional unauthorised interference to a computer system,	Please rephrase "intentional" intent to "dishonest" intent	We note that intentional intent is insufficient for attributing criminal

	program or data	Additionally, Section 6(5) should be amended so that only permanent modification which is serious enough, to warrant penal sanctions.	liability and we recommend that this offence should instead require dishonest intent.
Section 7 (1)	Unauthorised interception	We recommend addition of "serious physical injury" to prevent minor injuries from the scope of this section	This addition will cover other possible violations of human rights
Section 8	Illegal devices and access codes	We recommend removal of the exception giving 'sufficient' excuse or justification	This deletion prevents contradiction as the clause is directed towards actors with mens rea to commit a crime
Section 10	Enhanced penalty for offences involving a protected computer system	We recommend narrow and clear definitions of "computer system" and narrower powers of the cabinet secretary under Section 10 (2) (f)	ARTICLE 19 observes that this section provides for extremely harsh penalty that may have the effect of reducing computer use among citizens. In addition to that, section 10(2) (f) grants the Cabinet Secretary unrestricted power to designate other protected computer systems not enlisted in the list. We recommend that this power should be narrowed down to an objective criterion to be used in classifying

			additional protected computer system to this list.
Section 11	Cyber espionage	We recommend deletion of this section and amendments to the Penal Code and other acts applying to espionage	The provision as it is has a similar offline penalty and this new draft lacks the clarity and precision required of criminal laws and does not duly inform the citizens on which conduct is prohibited.
Section 12	False publications	We recommend deletion of this section	The terms "fictitious, false and misleading" are ambiguous and open to abuse by law enforcement officers and puts freedom of expression at jeopardy.
Section 13	Child pornography	We recommend deletion of this provision	We reiterate that child pornography is already dealt with under the sexual offences Act and this is merely a duplication of the same crime.
Section 14	Computer forgery	We recommend deleting the provision	Forgery is sufficiently covered under Penal Code
Section 16	Cyber stalking	We recommend deleting of this provision	The offese should be dealt with under other legislation which covers both online and offline as it is not clear what this phrase means 'repeated communication in the knowledge that this conduct will cause fear or detrimentally

			affect a person'.
Section 17	Aiding and abetting the commission of an offence	We recommend deletion of this section	This is sufficiently covered under other laws
Section 21	Crimes committed through the use of a Computer System	We recommend deletion of this section	The section would serve to discourage computer use and this would work against public interest.
Section 24	Investigating Procedures	We recommend deletion of this provision	The provision contradicts Article 24(2) and 31 of the Constitution.
Section 26 (6)	Investigating Procedures	We recommend deletion of this provision	ARTICLE 19 finds no public interest reason that warrants this extra-judicial procedure for the acquisition of a production order with respect to subscriber information and recommends that section 26(6) be removed in its entirety.
Section 28 and 29	Investigating Procedures	We recommend deletion of these provisions	We find the extended surveillance periods to go against international law and best practices
Section 38	International Cooperation	We recommend deletion of the provision especially as it provides for "without authorization"	The clause is open to abuse as it is and would allow disproportionate hacking

① D/Committees 14/2/18

Safaricom

Our Ref: R&PP/REVIEW OF LEGISLATION & REGULATIONS/Vol 1 13th February

The Clerk of the National Assembly
Office of the Clerk
Main Parliament Building
P.O. Box 41842-00100
Nairobi.

Dear Sir,

RE: **SAFARICOM'S SUBMISSION ON THE COMPUTER AND CYBERCRIME BILL, 2017.**

Please refer to the above matter.

We wish to express our gratitude to the Departmental Committee on ICT for the opportunity granted to us to present our views on the Computer and Cybercrimes Bill, 2017 (**"the Bill"**).

Please find enclosed herewith for the consideration of the Committee our Memorandum of Submissions, detailing our comments and suggested amendments to the Bill.

We trust that our submissions will be accorded due consideration and remain available to meet the honourable members of the Committee to further clarify our proposals.

Yours faithfully,
For: SAFARICOM LIMITED

Mercy Ndegwa
Head of Regulatory & Public Policy
Corporate Affairs

② EMEJEN pls deal FA 14/2/18

RECEIVED
13 FEB 2018
CLERK'S OFFICE

Safaricom Limited Submission to the Clerk of the National Assembly on the Computer and Cybercrimes Bill, 2017

	Title	Safaricom's Proposal	Justification/Comment
		PART 1- PRELIMINARY	
1.	Clause 7- Unauthorised Interception	Delete	It is an offence for a Telecommunications Service Provider to intercept their customers' communications. This provision therefore limits the fundamental right of privacy as provided in the Bill of Rights guaranteed by the Constitution of Kenya at Article 31. The Kenya Information and Communications Act Section 15, 31 and 83W further restrict Telecommunications Service Providers from monitoring, disclosing or allowing any person to monitor or disclose subscriber's communications. It is in violation of Section 15 of KICA.
2.	Clause 8- illegal devices and access codes	Amend to include all devices and access codes that may be used in committing offences under the Bill.	The current definition assumes that devices and codes used to perpetrate crimes are specifically created for the purpose of advancing criminal activities. Legitimate devices and codes may also be used to commit crimes. The bill does not expressly define illegal devices and access codes.
3.	Clause 13- Child Pornography	Widen the scope to include other sexual offences against children such as distributing explicit or subtle adult content whether visual, audio, text or in the form of digital literature to a minor, misleading a minor while engaging them online, as well as distributing content aimed at radicalizing a minor or distributing content that can spread fear and terror or undermines any rights and privileges that a child is entitled to under the Constitution of Kenya, 2010 and any other laws.	The definition of 'child pornography' as currently provided is limited and may not allow the prosecution of certain offences that are potentially pornographic. The proposal would be useful in enabling the Bill to achieve its objective of facilitating effective detection, investigation and prosecution of computer and cybercrimes.
4.	Clause 16 (3) (a)- Cyberstalking and Cyber-bullying	Delete	The clause provides an avenue for cyberstalking and cyber-bullying which are crimes under the Bill. The exception should be limited to law enforcement agencies under stringent controls.
		PART III-INVESTIGATION PROCEDURES	
5.	Clause 23 (1) (b)- Search and	Amend clause to read ".....the police officer or authorised person may apply to the court for issue of a warrant to enter any premises and with the assistance of a	It may be impractical and unnecessary for law enforcement officers to gain access to a private entity's business premises and its computer systems to search and extract data as this

	Title	Safaricom's Proposal	Justification/Comment
	seizure of stored computer data	principal officer or any person acting in a similar capacity, access, search and similarly seize such data...	may compromise its daily business operations. There are sufficient provisions that compel intermediaries to facilitate provision of data and co-operate with law enforcement agencies in investigations.
6.	Clause 23 (3)- Search and seizure of stored computer data	Amend clause to read "...the court shall issue a warrant authorizing a police officer or an authorised person, with the assistance of a principal officer or any person acting in a similar capacity to-...	As stated in no. 6 above, there are sufficient provisions that compel intermediaries to facilitate provision of data and co-operate with law enforcement agencies in investigations
7.	Clause 24- Power to search without a warrant in special circumstances	Provide more clarity and define what 'special circumstances' are.	The clause grants excessive powers to search and may be subject to abuse.
8.	Clause 26 (4)- Production Order	Delete	The clause is in conflict with Section 15 of the Kenya Information and Communications (Consumer Protection) Regulations, 2010 ("**the Regulations**") which require that a service provider maintain the confidentiality of a customer's information and communications. The regulations further provide that a service provider shall establish a mechanism through which a customer may know that information is being collected about them through their use of various telecommunications services and systems. Further, privacy is a constitutionally protected right and any limitation of this right ought to be disclosed to the affected person or persons.
9.	27(2)-Expedited Preservation and Partial Disclosure of Traffic Data	Amend to prescribe a defined period of preservation of traffic data. We propose a period of not more than thirty (30) days extendable for a further thirty (30) days as intimated in Clause 27 (3).	The requirement for a Service provider to preserve traffic data has no defined time limit. Traffic data cannot be held indefinitely.
10.	27 (4)-Expedited Preservation and Partial Disclosure of Traffic Data	Delete	The clause is in conflict with Section 15 of the Kenya Information and Communications (Consumer Protection) Regulations, 2010 ("**the Regulations**") which require that a service provider maintain the confidentiality of a customer's information and communications. The regulations further provide that a service provider shall establish a mechanism through which a customer may know that information is

	Title	Safaricom's Proposal	Justification/Comment
			being collected about them through their use of various telecommunications services and systems. Further, privacy is a constitutionally protected right and any limitation of this right ought to be disclosed to the affected person or persons.
11.	28 (1) (a)- Real time collection of traffic data	Amend clause to read "...permit the police officer or authorised person **acting through the assistance of a principal officer or any person acting in a similar capacity** to collect or record through..."	It is imperative that law enforcement enlist the assistance of persons conversant with the computer systems to avoid causing damage or preventing the entity from continuing to provide legitimate service to customers.
12.	29 (1) (b)- Interception of Content Data	Delete	The Constitution of Kenya at Article 31 guarantees every person the right to privacy and this includes the right not to have the privacy of their communications infringed. Clause 29 (1) (b) is in direct conflict with the provisions of the Constitution which is the supreme law of the land.
13.	29 (6)- Interception of content data	Delete	The clause requires that a service provider keep confidential an order to intercept and monitor content data. This is in conflict with Section 15 of the Kenya Information and Communications (Consumer Protection) Regulations, 2010 ("**the Regulations**") which require that a service provider maintain the confidentiality of a customer's information and communications. The regulations further provide that a service provider shall establish a mechanism through which a customer may know that information is being collected about them through their use of various telecommunications services and systems.
14.	29 (7) (a)- Interception of content data	Delete	The requirement is in contravention of existing legislation and may expose service providers to litigation.

THE COMPUTER AND CYBERCRIMES BILL, 2017

Consultative meeting with the Departmental Committee on Communication, Information an Innovation

Mr Joe Mucheru, EGH
Cabinet Secretary
Ministry of Information,
Communications & Technology

No	Current text	Proposal/Comments	Justification
			debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Kenya; "critical data" - to be provided.
2.	Section 24(1) Power to search without a warrant in special circumstances	(a) Define a criteria for situations that would meet the threshold for 'special circumstances	a. Waiver for the requirement for a warrant in advance of undertaking a search has the huge potential of infringing on constitutional rights an liberties, hence the need to be achieve with clarity circumstances under which this requirement would be waived in order to provide a an objective framework within which to evaluate applications. b. S. 24(2) - Section 119, 120 and 121 of the Criminal Procedure Code cited to serve as guidance are very removed from the reality of the speed and sophistication attendant to cybercrime and may need to be

No	Current text	Proposal/Comments	Justification
			infused with this reality.
3.	Section 41 Point of Contact	Delete 'and prosecuting cybercrime' from the third line as it creates a conflict of interest.	The point of contact should be the investigating agency only in order to promote independence of roles.
4.	General Comment		The success of implementation of this draft law will rest on a number of institutions, among them the NPS, NIS, CA, ICTA, KDF, ODPP etc. There is need to formalize a collaboration, and identify an appropriate agency empowered to handle the key elements of this law particularly the mutual legal assistance aspect.