RECEIVED
22 JUN 2018
CONSTITUTIONAL & HUMAN RIGHTS DIVISION

REPUBLIC OF KENYA
IN THE HIGH COURT OF KENYA AT NAIROBI
MILIMANI LAW COURTS
CONSTITUTIONAL AND HUMAN RIGHTS DIVISION
PETITION NO. 206 OF 2018

IN THE MATTER OF: **ARTICLE 2, 3, 20, 22, 23, 116, 165, 258 & 259 OF THE CONSTITUTION OF KENYA**

AND

IN THE MATTER OF: **THE ALLEGED CONTRAVENTION OF RIGHTS AND FUNDAMENTAL FREEDOMS UNDER ARTICLES 19, 21, 24, 25, 27, 28, 31, 33, 34, 35, 40 & 50 OF THE CONSTITUTION OF KENYA**

AND

IN THE MATTER OF: **THE ALLEGED CONTRAVENTION OF ARTICLES 1, 10, 118 & 238 OF THE CONSTITUTION OF KENYA, 2010**

AND

IN THE MATTER OF: **SECTIONS 3, 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 48, 49, 50, 51, 52 & 53 OF THE COMPUTER MISUSE AND CYBERCRIMES ACT**

AND

IN THE MATTER OF: **STANDING ORDERS 119, 127, 130, 131 & 133 OF THE NATIONAL ASSEMBLY STANDING ORDERS.**

BETWEEN

THE BLOGGERS ASSOCIATION OF KENYA (BAKE) ..... PETITIONER

VERSUS

THE HONOURABLE ATTORNEY GENERAL..... 1ST RESPONDENT

THE SPEAKER, NATIONAL ASSEMBLY..... 2ND RESPONDENT

THE INSPECTOR GENERAL OF THE
NATIONAL POLICE SERVICE. .....3RD RESPONDENT

THE DIRECTOR OF PUBLIC PROSECUTIONS.....4TH RESPONDENT

ARTICLE 19 EAST AFRICA.....1ST INTERESTED PARTY

KENYA UNION OF JOURNALISTS.....2ND INTERESTED PARTY

MUTEMI SUMBI
ADVOCATES
22 JUN 2018

3RD RESPONDENT'S REPLYING AFFIDAVIT

I, **JOSEPH KIPCHIRCHIR BOINNET, M.G.H. nsc (AU)**, the Inspector General, the National Police Service of the Republic of Kenya and of Post Office Box Number 44249 – 00100, Nairobi do hereby make an oath and state as follows:-

1. **THAT** I am conversant with the facts of this matter and I am therefore competent to swear this Affidavit.

2. **THAT** I swear this Affidavit in response to the Petition and Notice of Motion, both dated 29th May, 2018.

3. **THAT** in response to the Petition, it is of utmost importance that a background to the enactment of the **Computer Misuse and Cybercrimes Act, 2018 (the Act)** is provided.

4. **THAT** according to the Communications Authority of Kenya, internet penetration in Kenya is now estimated at 112.7% with 51.1 million Kenyans connected to the internet, the highest in Africa. Further, the total international internet bandwidth available in the country (Lit /Equip) is at 2,909.512 Gbps.

   Annexed hereto and marked JKB 1 is the Communication Authority of Kenya's First Quarter Sector Statistics Report For The Financial Year 2017/2018 (July-September 2017)

5. **THAT** this is a clear indication that more Kenyans now have access to the internet and are thus exposed to online risks and insecurity associated with the cyberspace. With the development of information and network technologies and the growing interconnectedness of the world, the risks connected to online communication have become increasingly pressing.

6. **THAT** on its part, mobile penetration is at 90.4 % with the number of active mobile money transfer subscriptions and registered agents stood at 28.1 million and 184,537 respectively. A total of 537.2 million transactions (sending and withdrawals) were made during the period valued at **Kshs. 1.65 trillion Kenya Shillings.**

7. **THAT** undoubtedly, the increase in mobile penetration in Kenya has resulted in a disruption in the manner in which trade and commerce is undertaken in the country. With such substantial amounts in transactions, the importance of creating a safe hub for the transfer of money cannot be gainsaid.

8. **THAT** cybercrimes is one of the most serious emerging threats to national security, law enforcement, private sector and individuals. The over 4 billion global internet users provide targets for cybercriminals.

9. **THAT** Cybercrimes are on an upward trajectory. A 2017 report by Cybersecurity Ventures found, among others that:

   a. The year 2017 saw the biggest cyber threat in recent history,
   b. Cybercrime is the greatest threat to every company in the world,
   c. Cybercriminal activity is one of the biggest problems that humanity will face in the next two decades.
   d. Cybercrime will cost the world in excess of USD 6 trillion annually by 2021, up from the current USD 3 trillion annually,
   e. Cybercrime will result in 'the greatest transfer of economic wealth in history, posing risks to the incentives for innovation and investment, and making it more profitable than global trade of all major illegal drugs combines.

Annexed hereto and marked JKB 2 is the 2017 Report by Cybersecurity Ventures.

10. **THAT** locally, cybercrime has resulted in destruction of data, theft of personal and financial data, embezzlement, fraud, reputational harm and lost productivity.

11. **THAT** Kenya is the worst affected by cybercrime in East Africa, with businesses being estimated to loss more than Ksh. 21 billion in 2017 (Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line- by Serianu). Further, Kenya recorded the highest percentage in Africa of people who have been affected, with 72% of the people affected.

Annexed hereto and marked JKB 3 is the Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line- by Serianu.

12. **THAT** Kenya has witnessed loss of lives as a result of cyber related offences, including cyber harassment/cyber bullying. Recent cases include a young person who committed suicide as a way of fulfilling the requirement of an online game known as "Blue-Whale Challenge" and a young lady who committed suicide in May 2017 following Facebook harassment.

See Pages 15 -16 of the Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line- by Serianu annexed as JKB 3 hereinabove

13. **THAT** in addition to loss of lives, child pornography is another malevolent offence that is targets children. The perpetrators of child pornography and other child exploitation offences are both from within and outside the country.

14. **THAT** cases of children and young women being exploited sexually, with nude photos and live recording of sexual intercourse, some with animals are rampant. Ensuing photos and videos are subsequently sold both locally and abroad.

15. **THAT** most recently, a United Kingdom citizen who was extradited from Kenya on sexual exploitation of children was convicted in the United Kingdom. The lack of cyber law in Kenya resulted in twenty (20) Kenyan witnesses giving evidence vide video link to a United Kingdom court despite the fact that his victims were all young Kenyan girls.

Annexed hereto and marked JKB 4 is the Kenya Online Child Exploitation Report, 2018.

16. **THAT** in November 2014, clandestine cybercrime labs were discovered in Gigiri, Nairobi. All the 87 suspects who were foreign nationals were later acquitted by the court. Their acquittal is attributed to lack of a legal framework to combat cybercrimes.

17. **THAT** cases of false information and disinformation have the potential of leading to lawlessness and anarchy. The International Covenant on Civil and Political Rights (ICCPR) recognises limitation of freedom of expression based on public order, among other grounds.

The wide use of social media poses a challenge to law enforcement in that messages spread very fast, and delay in conclusive attribution of source. Serious cases on misinformation have been reported during the electioneering campaigns, with a possibility of undermining democratic processes.

18. **THAT** moreover, cyber facilitated foreign interference with democratic processes, including in elections have been reported. The Office of the Director of National Intelligence in a report to the US president in January 2017 assessed that Russia conducted an extensive campaign to undermine the chances of Democratic candidate Hillary Clinton and to promote Republican candidate Donald Trump in the 2016 presidential elections, using both covert cyber attacks and overt efforts to influence public opinion. The obvious threat of this possibility happening in Kenyan democratic processes can only be mitigated with the enactment of the Act as currently enacted.

Annexed hereto and marked JKB 5 is a declassified version of the U.S. Office of the Director of National Intelligence report on Assessing Russian Activities and Intentions in Recent US Elections.

19. **THAT** prior to the enactment of the Act, the inadequacy of a cybercrime legal framework, resulted in the National Police Service opting to extradite suspects to other countries, with some suspects being jailed abroad for offences perpetrated in Kenya. In a recent case, Keith Moris, a British national who abused girls online and offline was arrested in Kenya and extradited to the United Kingdom due to lack of adequate legal framework in Kenya. Twenty (20) Kenyan witnesses gave evidence via video link to a UK court.

20. **THAT** further, cases of online terrorism related activities have been detected by the National Police Service with activities ranging from radicalisation, recruitment, and training. In **CR. 145/10/2013 R v. Liban Abdulle Omar** investigations conducted after the attack on the Westgate Mall in Nairobi divulged that the accused persons were coordinating their planning and attacks stages through social media networks that enabled them to accomplish their mission unnoticed. The legal authority to investigate such terror-related activities is contained in the Act.

Annexed hereto and marked JKB 6 is a report on cyber related cases from the Anti Terrorism Police Unit

21. **THAT** various businesses and individuals have been victims to cybercrimes as a result of a range of cybercrimes, ranging from electronic fraud, interception of communication, cybersquatting, fraudulent use of electronic data, issuance of false e-instructions among others.

22. **THAT** the speed of transfer and volatility of data calls for expedited preservation of data, which is to be subsequently used to protect lives and property, and subsequently used as evidence. Any delay in accessing and preserving data works to the advantage of criminals.

23. **THAT** wide reliance of internet/online services for government, communication, financial institution and other businesses, and for social purposes calls for a robust legal framework that ensures confidentiality, integrity, and availability of information, communication technology.

24. **THAT** it is these negative effects of cybercrimes that led to the National Police Service involvement in the process of enacting legislation to combat cybercrime, since the existing laws and investigative procedures are inadequate.

25. **THAT** indeed, cyberspace does not respect traditional state boundaries. Thus, the regulation of the cyberspace requires international cooperation. No State, regardless of its technological advancement, can singly effectively combat cybercrimes. Just like other countries, Kenya has an obligation to combat cybercrimes.

26. **THAT** most recently, in June 2018, the National Police Service received information from the Australia Federal Police regarding a case where an online chat account had been detected where people from foreign jurisdictions were connected with boys in Kenya for the purposes of sex tourism. A Kenyan suspect was arrested for the crime but the ability to investigate and prosecute the suspect has been severely undermined by the suspension of the Act.

27. **THAT** the Act was enacted in order to provide a framework to combat cybercrimes. The preamble of the Act states that the same **provides measures that enable timely and**

effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrime, facilitate international cooperation and related purposes.

THAT the Act was enacted at the behest of various government institutions including the National Police Service, businesses, the civil service and private individuals.

THAT the National Police Service was involved in the conception, drafting and discussion before and after publication of the various drafts of the Bill which was eventually adopted. Further, various government agencies, Kenyan institutions of higher learning, experts, including the 1st Interested Party herein were involved in the process of drafting the Act.

THAT therefore, all the offences created are matters that are of concern in combating cybercrime using the law enforcement approach.

THAT the 3rd Respondent therefore Prays that this Honourable Court dismisses the Petition with costs to the Respondents;

THAT what is deponed herein is true to the best of my knowledge, information and belief save what has been deponed to on information sources whereof have been disclosed.

SWORN at **NAIROBI** by the said]
JOSEPH KIPCHIRCHIR BOINNET]
this 20th day JUNE 2018]
]
BEFORE ME:]
]
]
]
]
]
COMMISSIONER FOR OATHS]

ERIC MURIMI KABURU
ADVOCATE
&
COMMISSIONER FOR OATHS
P.O. Box 105625 - 00101,
NAIROBI

DEPONENT

DRAWN & FILED BY:
T.A. NYAMODI & COMPANY
ADVOCATES
HSE NO 7 DUPLEX APARTMENTS,
LOWERHILL ROAD, UPPERHILL
PO BOX 51431-00200
NAIROBI
info@nyamodi.co.ke

[illegible]07/98
[illegible]017/512

[illegible] SERVED UPON

[illegible] SUMBI ADVOCATES
[illegible] 23, OFFICE NO. 2
[illegible]GURUONE ROAD, LAVINGTON
[illegible] BOX 2580-00202
[illegible]OBI
[illegible]2013/16; LSK/2018/01273

[illegible] OF THE ATTORNEY GENERAL
[illegible] HOUSE
[illegible]BEE AVENUE
[illegible] BOX 40112 – 00100
[illegible]OBI.

[illegible]EAKER OF THE NATIONAL ASSEMBLY
[illegible]AMENT BUILDINGS
[illegible]OBI

[illegible] OF THE DIRECTOR OF PUBLIC PROSECUTIONS
[illegible] BUILDING, BLOCK A, 19TH FLOOR
[illegible]OBI

THIS IS THE EXHIBIT MARKED "JKB-01"
REFERRED TO IN THE ANNEXED AFFIDAVIT
/DECLARATION OF JOSEPH KIPCHIRCHIR BOINNET
SWORN/DECLARED BEFORE ME ON THIS
20TH DAY OF JUNE 2018 AT
NAIROBI IN THE REPUBLIC OF KENYA

COMMISSIONER FOR OATHS

COMMUNICATIONS AUTHORITY OF KENYA

FIRST QUARTER SECTOR STATISTICS REPORT FOR THE FINANCIAL YEAR 2017/2018 (JULY-SEPTEMBER 2017)

Direct any queries on the report to:
Director/Competition, Tariffs and Market Analysis
Tel:+254-703 042000, +254 - 713 172000
Email: info@ca.go.ke
Website: www.ca.go.ke

***Disclaimer*:**
Although every effort has been made to ensure accuracy of the data contained in this report, the Authority is not liable for inaccuracies in any of the information contained in this report, which is contingent upon the operators/service providers' compliance returns.