1ST Floor
Coffee Nicol House
49 Siaka Stevens Street
Sierra Leone
(+232)79601556
(+232)76140723
(+232)76757677

FIAT JUSTITIA Email: barassociationsl@gmail.com

23rd April 2021

POSITION PAPER ON THE CYBERCRIME BILL 2020

The quantum leap of ICT infrastructure and the continuous revolution and dynamism of its systems demand proper regulation of the same. In this regard the Sierra Leone Bar Association (hereinafter referred to as 'SLBA') shares the view of the International Telecommunications Union that clear steps have to be taken by governments with regards these matters and commends the Government for taking the lead in this area. We applaud the call by Parliament for proper public debate to scrutinize this important piece of legislation and we consider it essential that before the passage of a bill regulating cyberspace, the citizenry's view should be fullyventilated to encapsulate our collective aspirations for free but responsible use of cyberspacewhilst ensuring respect for and protection of fundamental human rights.

SLBA has had some fruitful consultations with the Government through the Ministry of Information and Communications who obliged us the draft bill and some supporting documentation for our comments.

Our views with regard the bill are geared towards ensuring proportionality, reasonability, pragmatism, and safeguards for citizens' rights. In addition, the Association's positions are informed by our review of best practices from other jurisdictions in Africa and the wider world with regard to both cybersecurity frameworks and the protection of human rights. Our recommendations and suggestions are meant to address areas of concern with a view to enrich the Bill's contents to meet itsstated overall objectives.

The suggested changes inserted into the Billare in blue characters and are the principal changes we wish to be considered and incorporated into the Bill for enactment.

1. THE ENACTMENT OF A DATA PROTECTION LAW

The full operations and ethos of the legislation would mean the collection of huge volumes of data overtime and the absence of a data protection law to go hand in glove with cyberspace regulation

service providers and users' right to privacy and freedom of speech, the misuse or improper use and interference with the data collected could undermine the entire vision behind this commendable venture. We therefore call on the Government to urgently enact a data protection legislation to support its desired implementation of the cyberspace regulation.

2. CHANGE OF BILL TITLE TO CYBERSECURITY ACT

The rationale underpinning the legislation is to make provision for the use of cyberspace, ensure protection and safety of users, regulations, assessment, fostering international cooperation, enforcing noncompliance of regulations and laws and applying sanctions in the case of violations. To title the bill "Cybercrime" without more informs that what is sought is retribution in relation to the use of cyberspace systems which we do not believe is the intention of the government and/or its partners. We therefore recommend that the legislation be titled "Cybersecurity Act" or alternatively "Cybersecurity and Cybercrime Act" as was done by the Republic of South Africa.

3. DEFINITION OF TERMS

We have added definitions of several terms into the relevant section for a better or more uniform understanding of the Bill. Significant amongst these are "*enforcement officer*", "*false news*", "*seize*" and "*subscriber information*". The change to enforcement officer in particular elevates responsibility for the enforcement of the provisions of the Bill from just any police officer to "*an officer in a law enforcement agency trained in cyber security work designated or authorized to carry out functions including for the purposes of Part III of this Act.*"

4. INTRODUCTION OF CAVEATS

Our draft also now introduces a couple of caveats including viz the application of the Act:

i. Evidence obtained can be used in a trial only if "*it has been properly obtained and preserved.*"
ii. That rather than the enforcement officer relying on his own subjective belief having had "*reason to believe*", we have suggested he has "*reasonable grounds to believe*" which informs of an objective standard by which the enforcement officer's conduct would be assessed.
iii. Warrants obtained under the Act may be set aside upon an application by a person affected to a Judge of the High Court and

this includes service providers under section 7(7) of the redrafted Bill.

In light of this kickback provision granted to service providers, the Bill also now states that if they "*without reasonable excuse*" fail to comply with an order with regard the collection of real time data, they would be liable to sanctions. This mental element is significant in ensuring that whilst provision is made for their input in the effective regulation of the use of cyberspace, they also do not misuse this leeway granted to them.

These specific suggestions ensure that service providers have some say in the handing out of customer information. But on the whole, the suggestions are geared towards balancing the rights and interests of the subjects as against the need to ensure enforcement of the provisions of the Bill, creating a system of checks and balances.

5. INSERTION OF QUALIFIERS

Our draft has suggested parameters on which a court may grant an application for a search and seize warrant. We have also inserted qualifiers with regards 'searches and seizures' which now require not just "*a reasonable ground of belief*" but a statement of the "*specific scope of the belief and the scope of the warrant required*". This heightened requirement is to ensure that any infringement of a person's right is reasonably justifiable and is subject to respect for his/her fundamental rights.

6. SPECIFICITY OF THE PENALTIES/ENFORCEMENT REGIME

In addition, authority to met out punishment is no longer arbitrarily vested in the hands of the Minister of Information and Communications but is now specified under the Act for all parties involved including enforcement officers who may want to misuse their powers.

It is important to note that the remedies under the Act as proposed by us, will include both civil and criminal sanctions which also informs why the Bill should be titled "Cybersecurity".

7. STANDARDS, POLICIES AND GUIDELINES

We have also inserted into the redrafted bill and would suggest the incorporation of the same into the Act, certain roles for the National Computer Security Incidence Response Team in section 6(5) in regard the making of standards, guidelines and polices for the proper and effective operation of the Act.

8. MONITORING TIMEFRAMES

We also suggest that the provisions in the Bill stipulating a timeframe of 90 days be shortened to 30 days which may be extended by the Court for a reasonable period of time, the same not to cumulatively exceed 60 days.

9. SAFEGUARD OF DATA COLLECTED

Section 10(h) has been added to ensure that an application for data to be intercepted should show that there are adequate provisions in place to ensure the safe storage and protection of the content obtained and that they are to be used solely for matters relating to the investigations.

10. NEW PROVISIONS

We also suggest and have included into the draft bill 3 new sections under the rubric of Territorial Jurisdiction to wit:

i. Section 13 gives all law enforcement agencies the power to prosecute offences under the Act except in instances where leave of the Attorney-General has to be sought.
ii. Section 14 guides the court on the sort of sentences it may impose including but not limited to the confiscation of assets, and significantly what is to become of them.
iii. Section 15 gives additional guidelines particularly within the remit of false pretences or fraud.

This means that the numbering of the sections in the draft bill has changed to accommodate these provisions, after which the numbers in the original Bill would move three steps down.

11. ACCESS TO DATA WITHOUT AUTHORISATION

In section 28, we have inserted into the Bill for consideration the circumstances in which an enforcement officer may access data without authorisation; and have suggested that this be "*only in exceptional circumstances and when reasonably necessary*". This however goes with the proviso that such access may be rescinded by the Court upon an application by a person affected.

12. AVOIDANCE OF STRICT LIABILITY

We have in various sections introduced a mental element into the Act to avoid the inadvertent creation of strict liability offences. In section 36, we suggest and have inserted the word "*adversely*", the

word "*wilfully*" in section 5(9) and "*intentionally, recklessly or negligently*" in section 5(8) so that a punishable infraction is deliberate. This ensures that innocent acts or acts done with reasonable excuse do not inform a criminal conviction. The addition in section 5(9) particularly ensures that enforcement officers are held accountable for unauthorised, unlawful leaks of data collected.

13. SYCHRONISATION WITH EXISTING LEGISLATIONS AND MENTAL ELEMENT

With regard cyberbullying and cyberstalking in section 39 of the Bill, we suggest and have inserted a phrase that the provision is without prejudice to what is currently contained in the Domestic Violence Act 2007 and the Sexual Offences Act 2021 and in subsection (2) thereof "*intentionally or recklessly*". This is meant to offer effective protection to the victims whilst also ensuring respect for the rights of the accused persons.

14. AIDING AND ABETTING

For the punishment in this regard, we suggest and have inserted that it be the same for persons found guilty as the punishment prescribed for the substantive offence to which the aiding and abetting relates. This brings it into consistency with the criminal law statutes in our laws.

15. RACIST AND XENOPHOBIC ETC. OFFENCES

In the case of racist and xenophobic etc. offences, we suggest and have inserted the words "*gender*" and "*disability*" to ensure the provision is all encompassing and inclusive.

16. WINDING UP OF ENTITIES

With regard the power to wind up entities and asset forfeitures, we suggest and have inserted for incorporation words that inform that the sanctions shall only be imposed in circumstances which threaten national security and in the case of multiple and repeated offenders, any forfeiture of assets would be made after they have satisfied their liability owed to other persons. This ensures a balance is struck between the need to protect the State and the rights of persons that could be adversely affected by such sanctions.

17. ACTS BY CHILDREN

We have inserted and will suggest for incorporation the following new section to wit:

"Without prejudice to the offences prescribed under this Act and subject to the provisions of the Children and Young Persons Act Cap.44 and the Child Rights Act 2007, where an act done by a child would be deemed to be an offence under this Act such child shall be treated as a juvenile and dealt with accordingly".

To address acts by children and to ensure that whilst some form of punishment could be meted out for such acts, the punishment if any should be in accordance with the law relating to the treatment of children and young persons. The rationale of this bill is not to criminalise the common and relatively normal behavior of children of this era. If we fail to address this at this point, we will create a generation in which criminality becomes the norm. Our review of contemporary approaches of cybercrime inform that advanced countries with enriched cyberspace regulations are currently being confronted with the conundrum of dealing with cyberacts done by children and how to address the same. This section therefore represents an innovative and forward thinking approach to address the problem so that at the onset of the introduction of cyber law in Sierra Leone adequate provision is made.

18. NATIONAL CYBERSECURITY ADVISORY COUNCIL

On the Chairmanship of the Council we suggest and have inserted for incorporation that the same be occupied by the Minister responsible for internal affairs. While we note his Excellency the President is commander in chief, our experience informs that operational issues of such nature should be left in the hands of persons who on a day to day basis deal with the security sector.

With regard to the members of the Council we suggested and have inserted for consideration the provision of four (4) positions from the general public to wit;

i. a representative of the paramount chiefs, to ensure full community and local participation of our traditional leaders for complete and unfettered acceptability of the bill;
ii. a person with a respectable distinguished career and background in ICT and related matters;
iii. a representative of the SLBA of over 15 years post enrolment at the bar and
iv. a respected and distinguished member of the Sierra Leone society appointed by the President.

This would strike a balance in representation and ensure acceptability and compliance with the law.

In regard the terms of the Council members, we suggest and have inserted for consideration the following:

a. he ceases to hold membership if he loses the office on the basis of which he became a member of the Council or for stated misconduct or infirmity of body or mind.
b. in the case of non political appointees, they shall cease to hold office only for stated misconduct or infirmity of body or mind for a term of 5 years which said term shall where the President deems fit be renewed for a further term of 5 years without any further renewal.

CONCLUSION

We call on the Government to adopt our recommendations and suggestions and subsequently continue on this path for inclusive transparent and public consultative processes.

Osman Jalloh Esq.
Chairman/Team Lead
Sierra Leone Bar Association
Cyber Bill Review Committee

Abdul Karim Koroma
General Secretary
Sierra Leone Bar Association

Eddinia Michaela Swallow (Ms.)
President
Sierra Leone Bar Association