Confidential Submissions.

19 June 2020.

The Standing Committee on Justice, Law and Human Rights
Parliament of the Republic of Fiji,
Government Buildings,
Suva,
Fiji Islands.

Sent via email to : ira.komaisavai@parliament.gov.fj

Dear Chair,

ICT SUBMISSION - Cybercrime Bill 2020
Bill No. 11 of 2020.

We thank the Government of the Fiji Islands, Fijian Parliament and more particularly the Parliamentary Standing Committee on Justice, Law and Human Rights ("**Committee**") for enabling this dialogue regarding very important legislation for the protection of the people of Fiji.

Your humble contributors are persons with expertise in the Information and Communication Technology and Internet Governance space who wish to provide useful information for the Committees consideration. This is to ensure the resultant legislation is theoretically sound according to the Council of Europe Convention on Cybercrime (Budapest Cybercrime Convention) but also practical for the service of Fijians in the country.

These were our collective views from a short two (2) hour meeting of 16 June 2020, but if we had more time to present verbally and directly with a division of the relevant Ministry we would be happy to do so for full review.

Although discussions were conducted in 2015 and 2016 technology has changed very much indeed in the last four (4) years with respect to blockchain, encryption, artificial intelligence (AI) and other technologies – hence a need to look in light of changes since.

Within the time allowed over the last 7 days though, our preliminary views are as follows :-

Scope.

1. We fully agree that coverage should and must cover those actions which are conducted by cybercriminals outside of the Fiji Islands. The coverage of the legislation in Subsection 3 (2) (a) (ii) seems to be broad enough accordingly :-

   "…*a result of the conduct constituting the alleged offence occurs in Fiji*."

2. Regarding Subsection 3 (2) (b) the requirement for a ship to be flying the flag of Fiji to be caught by the legislation may be an issue if they are a yacht for example conducting illegal distribution of child pornography from our islands, but cannot be caught due to the flag requirement.

3. Possibly the definition of "Computer System" should also encompass things which are capable of being connected to a Computer System or Computer Program. This could be done by a wider definition of "Electronic System". Based on the current definition we were not clear whether tampering with E-Ticketing or EftPoS cards using things like a Card Skimmer or Near Field Card readers would apply.

Definition of Service Provider.

4. The definition of service provider in our view is wide and whilst subsection (a) does broadly make sense, the subsection (b) expands this too wide as to possibly include every agency including the Parliament of Fiji as a "service provider" as it expands to an entity which even stores data for others. See below and underlined.

5. Whilst we agree service providers should include :-
    a. **Telecommunication Operators** such as Telecom Fiji, Vodafone and Digicel respectively as well as
    b. **Content / Over the Top ("OTT")** providers such as imo.im, viber and facebook messenger – we do not believe this should be so wide as to encompass any entity with a server.

    ""*service provider" means—*
    (a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or
    (b) any other entity that processes or stores computer data on behalf of the entity or users of such service provided by the entity;"

6. We would be happy to discuss a definition with the operative Ministry to ensure that only "*service providers*" are applied.

Resources for Implementation :

7. There is currently a definition of "Authorised Person" to only be a ***Fiji Independent Commission Against Corruption Act 2007*** officer, but later the legislation refers to Police and ***Crimes Act 2009***. Potentially the Authorised Persons can include any party currently able to seek Search Warrant under their respective legislations including Fiji Revenue Customs, Financial Intelligence Unit, FICAC, the Police, CID and others.

8. We note though that each of these Parties might not be able to properly articulate, log nor resolve Cybersecurity issues in the country. Even in small countries a Computer Emergency Response Team ("CERT") can be put in place as a buffer to clearly articulate a needs analysis and block Cybersecurity threats from abroad.

9. From a Financial Services standpoint the Financial Intelligence Unit could be a key point of contact also.

10. This legislation presently only allows our current bodies to implement this legislation, but there is not a technical body such a CERT which proactively plugs these gaps, then becomes an advisory body to inform the following stakeholders of what the issues were and how to stay away from danger :-
    a. the Fijian Public.
    b. Service Providers.
    c. Large Organizations, especially financial institutions.

Offences.

11. As those with expertise in the industry we reviewed common cybersecurity threats and where they might sit in the current version of the legislation. Though we have only had limited time to review we attach this as ***Annex 1*** hereto.

12. We note that the version submitted for consultation here as provided by the Parliament of the Republic of Fiji Facebook page URL " *Download copy of the Cybercrime Bill - https://bit.ly/3f27v4q* " does not have the former Section 11 with respect to Child Pornography. We strongly believe that Child Pornography is an area which should be included unless it is already provided for under other legislation on similar terms.

13. If the offence of Child Pornography is included back then reference should also be made to the definition of "Child" in the other relevant legislation.

14. With respect to penalties for crimes there should clearly be a requirement for :-
    a. restitution as penalties between F$10,000 and F$50,000 is not sufficient if a Cybercriminal has stolen millions from a banking institution (for instance).
    b. Perhaps there needs to be a threshold for higher fines in some instances, but given timeframe restrictions we will need to understand this better before making further and better submissions.
    c. Guidance can also be had by way of Financial Transaction Act penalties with similar levels of risk if financial services are subject to hacking (as an example). Those would most definitely be at a higher threshold.

15. We see that "Aiding and Abetting" is only clearly set out in Sections 11 and 12 with respect to Part 4 – Other Offences, but aiding and abetting should be covered across all offence.

Service Provider Interception Options.

16. There are two matters which make Section 22 (6) in current draft *Real-time collection of traffic data* and Section 23 *Interception of content data* which requires Service Providers (which needs some clarity as above) would be very difficult to implement or possibly impossible as:-
    d. content, platform or OTT providers would be the only parties with unlock keys to the encryption across ; and
    e. individuals are able to use Virtual Private Networks or VPN services to spoof their IP address location.

17. Dealing with each technology in turn, when a consumer (in or outside of Fiji) enters data into a website with https coding the "s" at the end denotes that it is a secure site which encrypts data. This is clearly a good thing as it allows fair and safe transmission of credit card details. If service providers could see this then some nefarious parties within such operations could see such details to take money.

18. Furthermore blockchain technologies and even OTT's such as viber, facebook messenger and imo.im use encryption – so even if a Service Provider were able to look beyond the curtain into data being sent, it would be in a format they could not see without the service provider providing the "key". Facebook or Viber providing us with the key is very unlikely.

19. Secondly a VPN or Virtual Private Network can make a Fiji user create a secure (encrypted) connection which appears in another country and IP spoofing is used and Internet Protocol packets with a false source IP address, for the purpose of impersonating another computing system. This is inexpensive technology which can be downloaded through software online.

20. This can be used for various uses such as allowing a consumer to appear they are accessing the internet from the United States so they can watch the United States version of Netflix (with far more channels) or Disney+ webstreaming services which is not available in Fiji. But at the same time it can be used to hide details which make it impractical or impossible to implement Sections 22 and 23.

We would be happy to discuss the technical aspects and practicalities around our submissions should further consultation allow.

Those within the ICT industry are usually willing to assist with awareness towards general consumers as well as SME's around the country. To that end, once the legislation is finalized we would welcome collaboration with the relevant Ministries on how we could work together for the best interests of the Fijian people.

Yours Sincerely,

Anju Mangal As a private citizen. 15+ years in the ICT industry.	Cherie Lagakali As a private citizen. 10+ years in the ICT industry.	Georgina Sakimi-Naigulevu As a private citizen. 10+ years in the ICT industry.
Andrew Naigulevu As a private citizen. 10+ years in ICT Industry.	Kunal Singh As a private citizen. 5+ years in the ICT industry.	Peter Rigamoto As a private citizen. 10 years in the Telecommunications Industry.
Esira Kini As a private citizen. 10 years in Financial Services Sector.	Amit Singh As a private citizen. 20 years in the ICT industry.	

Contactable via Email : gisakimi@gmail.com

ANNEX 1 :

TECHNICAL ATTACKS vs OFFENCES IN BILLS.

Type of Attack.	*Where this might be in current version of Bill.*
Denial of Sservice	Australia "Unauthorised impairment of electronic communication." Fiji Bill – Section 7 perhaps.
Phishing	Australia "*general dishonesty*" or "*by deception*". Potentially in current version Section 11 which is Identity Theft.
Hacking	Australia "*possession or control of data with intent to commit a computer offence*" which requires (i) control and (ii) use for offence. Fiji Bill - Part 2.
Identity Theft.	Potentially in current version Section 11 which is Identity Theft [alternate version Section 12].
Electronic Theft.	Fiji Bill - Part 3.
Child Pornography.	Was formerly Fiji Bill - Section 11. To be included back.
Other Pornography.	Not dealt with here but is within Online Safety Act 2018 (Fiji) section 23.
Viruses.	Fiji Bill – Section 8. Regarding computer program for an offence.
Terrorism.	Speech related offences which are now prohibited in Aust / NZ / Samoa with regards to terrorism are not currently present.
Defamation.	Not dealt with here but potentially within "causing harm" provisions of the Online Safety Act 2018 (Fiji) section 24. Not present.
Blockchain and Encryption?	Wondering whether s22(1)(b)(iv) on stored data for decryption information is to cover this aspect. Not present.
Skimmers	Not present.