20th June 2020

"By Email"

The Chair
Standing Committee on Justice, Law and Human Rights
Parliament of the Republic of Fiji
Suva
FIJI

Re: Submission on the Cyber Crime Bill No. 11 of 2020

Dear Hon. Chair,

1. Firstly, I would like to congratulate the Committee in inviting us to comment on the Bill in its current form.
2. Thank you for the opportunity to comment on the Cyber Crime Bill No. 11 of 2020.
3. The Committee and Parliament needs to ensure that there is adequate law to penalize cyber offences because there are gaps in the current legislation.
4. Cybercrime takes place online. There are two overarching areas of cybercrime:
    - cyber-dependent crime - which can only be committed through the use of online devices and where the devices are both the tool to commit the crime and the target of the crime, and
    - cyber-enabled crime - traditional crimes which can be increased in scale by using computers.

5. I would like to submit a paper I wrote in 2010 called Cyber Security in the Republic of Fiji where on pages 13 and 14, I made a comparative analysis of various jurisdictions' cyber crime offences. I have revised that Table and am submitting it here to factor in the *Online Safety Act 2018* of Fiji and the UK's categorization of cyber crime.
6. The *Online Safety Act 2018* is primarily based on a subset of content related offences and is general and just points to harm which is why "grooming" in my view where an adult seduces children needs to be canvassed.
7. In relation to the (13) of the UK's categorization, I do not think that needs to be put in the legislation as it could potentially harm access to content by village schools that may not have adequate libraries but have access to virtual libraries and content and personally feel that the "fraud" provisions that already exist in Fiji's *Crime's Act* will suffice.
8. For ease of your analysis, I have updated the Table in my submission, which I have shared below to assist the committee in identifying the lacunas that still exist.
9. I look forward to making verbal submissions to you on Thursday at 10:30am.

Comments on the Bill in its current Draft:

Commentary on certain words within the Interpretation section

In terms of the Interpretation Provision, kindly find my commentary and I also offer some context for my recommendations:

10. "Authorised person" should also include those at the Office of the Director of Public Prosecution and the Online Safety

Commission and in the future where a body is created specifically to deal with this. I would widen this from “police officer” to “law enforcement officer.”

11. “Minister” should be the Minister of Defence as Cyber Crime Policing is a law enforcement issue. The Ministry of Communication is responsible for setting Policies and regulating telecommunications and the internet but it is the Police that enforces the law and the Police come under the Ministry of Defence. To understand cooperation within the legislative Framework, see illustration below and refer to pages 11-13 of Cyber Security in the Republic of Fiji 2010.

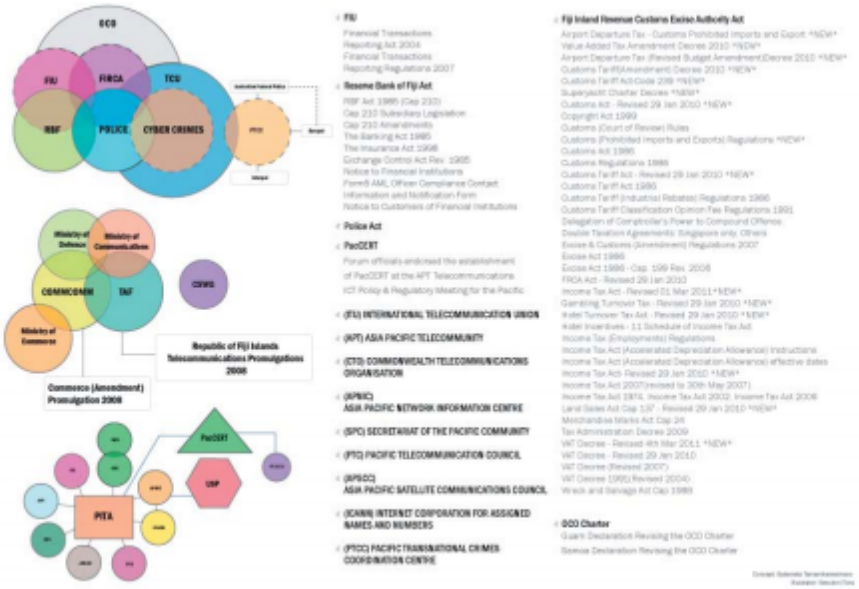

Figure 7. Illustration showing cybersecurity regulatory environment in Fiji.

Illustration by Salanieta Tamanikaiwaimaro (2010)

12. “serious offence” – the damages caused by certain cyber crime can amount to millions of dollars in damages and

certainly way more damages than $500 and 6 months imprisonment. Over the years, whilst we were conducting nationwide consultations, there were many victims who incurred aggravated damages. Serious offences are usually indictable by 5 years. There needs to be a distinction between what are *summary offences*, *either way offences* and *indictable offences*. This is to ensure that children and others who may be first offenders are given an opportunity to rehabilitate without a permanent record.

13. “Service Provider” definition should be expanded to include an entity that provides access to the Physical Layer, Transportation Layer or Application Layer of the Internet. The rationale for this is interference along fibre cables, theft of telecommunication services do not necessarily occur within computers but within the wider cyber environment which consists primarily of the three layers. The Application layer also includes things like ATM machines etc. To illustrate the same, see image below:

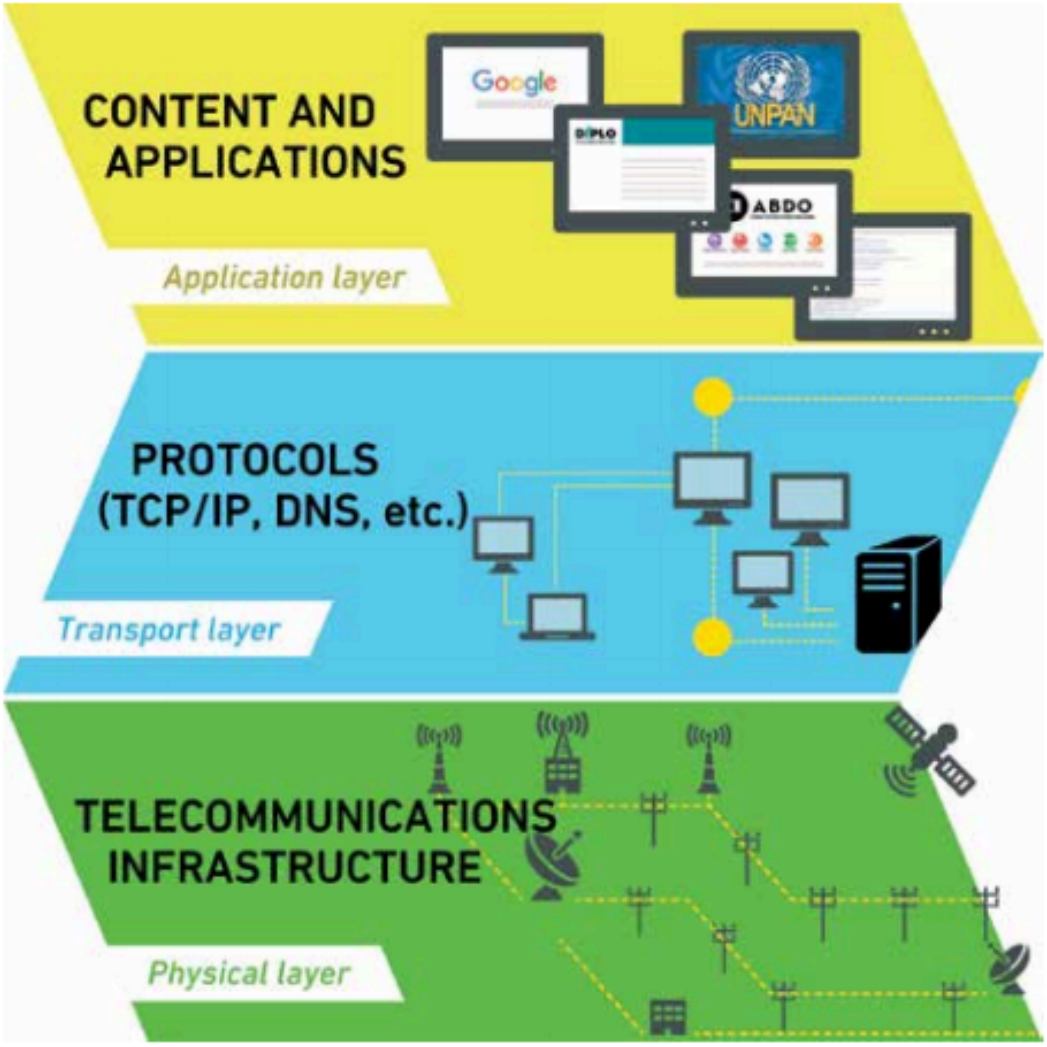

Illustration is from pg. 35 of An Introduction to Internet Governance 7th edition (Kurbalija, J).

It is important to note that in order to adequately prosecute theft of telecommunication services, espionage in submarine cables etc, it is important to adequately identify the cyber environment, which can be on the internet or closed within an intranet.

For context, the “Internet relies on the telecommunications infrastructure as the medium through which the traffic flows: cables such as copper wires or optical fibres; electromagnetic waves such as satellite, wireless links, and mobile networks.

In many cases, the existing telecommunications infrastructure – such as the telephone lines and mobile connectivity, power grid, undersea cables, or satellite links – is utilised to carry Internet packages. Increasingly, an innovative telecommunications infrastructure is being deployed to carry data – such as high-bandwidth submarine fibre optic cables, fifth-generation (5G) mobile networks, and innovative wireless solutions like Google balloons4 or Television White Spaces,5 as well as technologies enabling greater deployment of the IoT" (Kurbalija,J. 2016. An Introduction to Internet Governance, 7th Edition).

14. "Traffic data" need not be limited to being generated by a computer system so that illicit and harmful activities that do not necessarily originate from a computer would rule out various other offendings. I would also suggest changing the wording to "any data" instead of limiting it to "computer data".

Commentary on s.3 of the Bill (Application)

15. Cyber attacks can be committed from a "long geographical distance, and can also be done anonymously. By nature, cyber crime has a transborder nature that makes it harder to track and investigate" and restricting it to "Fiji citizens" and "Fijian jurisdiction" restricts the country's capacity to prosecute offenders abroad. Even the use of the word "not"….in the "whether or not" is ambiguous and criminal law has to be precise to enable prosecution to prove the offence and defence to defend the allegations and charges.

(Kunnapu, M.2007. Estonian Cybercrime Legislation and Case Law Responses to the 2007 Cyber Attacks)

16. There are several offences that are not covered by the Cyber Crime Bill and these are in **orange** in the table below which is an updated version of what I refer to in my paper which I mentioned above that is also attached. Please refer to the Table below which is annexed herewith.

Yours faithfully,

Salanieta Tamanikaiwaimaro

Annexure Table Showing Categories of Cyber Crime by Jurisdiction and Comparison to Fiji's categorisations

EU's CYBER CRIME CONVENTION CATEGORIES	FIJI's DOMESTIC LAWS	CYBER CRIME BILL NO.11 of 2020
1. Crimes against the Confidentiality, Integrity and Availability of computer data and systems	s.340 -s.346 Crimes Decree 2009	s.5-8.
2. Computer related traditional crimes	s.340 -s.346 Crimes Decree 2009	
3. Content-related offences	S24, S25 Online Safety Act 2018	
4. Offences related to infringement of copyright and related rights		
5. Infringement of privacy	s12,s14 of Compulsory Registration of Customers for Telephones Services Decree 2010	
AUSTRALIAN INSTITUTE OF CRIMINOLOGY's CATEGORISATION OF CYBER CRIME		
1. Theft of Telecommunication Services;		s.12
2. Communications in Furtherance of Criminal Conspiracies;		
3. Telecommunications Piracy;	s2 Copyright (Amendment) Decree 2009	
4. Dissemination of Offensive Materials;	S24, S25 Online Safety Act 2018	
5. Electronic Money Laundering and Tax Evasion;	Customs Act, Customs Tariff Act, Excise Act, Gambling Turnover Decree, Income Tax Act, Land Sales Act, Merchandise Marks Act, Value Added Tax Decree, Wreck and Salvage Act	
6. Electronic Vandalism, Terrorism and Extortion;		

7. Sales and Investment Fraud;	s317, 318 Crimes Decree 2009	
8. Illegal Interception of Telecommunications;		
9. Electronic Funds Transfer Fraud		
UNITED STATES DPT OF JUSTICE CATEGORISATION OF COMPUTER CRIMES		
1. Obtaining National Security Information;		
2. Compromising the Confidentiality of a Computer;	s.340 -s.346 Crimes Decree 2009	
3. Trespassing in a Government Computer;	s.340 -s.346 Crimes Decree 2009	
4. Accessing a Computer to Defraud and Obtain Value;	s.340 -s.346 Crimes Decree 2009	
5. Knowing Transmission and Intentional Damage;		
6. Intentional Access and Reckless Damage;		
7. Intentional Access and Damage;		
8. Trafficking in Passwords;		
9. Extortion Involving Threats to Damage Computer.		
UNITED KINGDOM COMPUTER MISUSE ACT 1990, MALICIOUS COMMUNICATION ACT 1988, COMMUNICATIONS ACT 2003		
1. Hacking		s.5-8.
2. Malicious Software		s.5-8.
3. Distributed Denial of Service Attacks		
4. Dark Web		
5. Trolling	S24 Online Safety Act 2018	
6. Online Threats	S24 Online Safety Act 2018	
7. Disclosure of private sexual images without consent	S24, S25 Online Safety Act 2018	
8. Grooming	S24 Online Safety Act 2018	
9. Stalking Online	S24 Online Safety Act 2018	
10. Virtual Mobbing	S24 Online Safety Act 2018	
11. Phishing	S24 Online Safety Act 2018	
12. Identity Theft		s.11

13. Using the Internet to carry out intellectual property fraud, counterfeit goods either billed as genuine or fake, counterfeit , setting up or running websites purporting to be genuine retail outlets, streaming content owned by someone else online for example a new cinema release or live sports matches		