[VERBATIM REPORT]

STANDING COMMITTEE ON JUSTICE, LAW & HUMAN RIGHTS

BILL

Cybercrime Bill 2020 (Bill No. 11 of 2020)

INSTITUTIONS:
(1) Digicel Pacific Group
(2) Office of the United Nations High Commissioner for Human Rights
(3) United Nations Office on Drugs and Crime (UNODC)

VENUE: Big Committee Room - East Wing, Parliament Precincts, Government Buildings.

DATE: Wednesday, 24th June, 2020

VERBATIM NOTES OF THE VIRTUAL MEETING OF THE STANDING COMMITTEE ON JUSTICE, LAW AND HUMAN RIGHTS VIEWED AT THE BIG COMMITTEE ROOM, EAST WING, PARLIAMENT PRECINTS, GOVERNMENT BUILDINGS, SUVA, ON WEDNESDAY, 24TH JUNE, 2020 AT 9.20 A.M.

Online Interviewee/Submittee: Digicel Pacific Group

In Attendance:

1. Mr. Peter Rigamoto - Head of Legal (Pacific Hub)

MR. CHAIRMAN.- Thank you, Honourable Members, members of the media and the general public, the secretariat team, viewers, ladies and gentlemen. A very good morning to you all and those who are actually watching this live telecast from the comfort of their homes. It is a pleasure to welcome everyone, especially the viewers who are watching this session.

For your information, pursuant to Standing Oder 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the general public. Therefore, please note that this public hearing is open to the public and media, and is also being aired live on television via the Parliament Channel on the Walesi Platform and Parliament website.

For any sensitive information concerning this inquiry that cannot be disclosed in public, this can be provided to the Committee either in private or in writing. However, please be advised that pursuant to Standing Order 111, there are only few specific circumstances that allow for non-disclosure which include:

- national security matters;
- third party confidential information;
- personnel or human resources matters; and
- deliberation and development of Committee recommendations and reports.

At the outset, I wish to remind Honourable Members and our Witness, that all questions to be asked are to be addressed through the Chair. This is a Parliamentary inquiry and all information gathered is covered under the Parliament Powers and Privileges Act.

In terms of the protocol of this Committee hearing, please be advised that there will be no usage of mobile phones. All mobile phones are to be on silent mode while the meeting is in progress.

I would now like to introduce Honourable Members of the Committee.

(Introduction of Committee Members)

Today, the Committee will be hearing submission on the Cybercrime Bill 2020 (Bill No. 11 of 2020). As everyone is aware, this Bill was introduced under Standing Order 51 and was referred to the Standing Committee on Justice, Law and Human Rights to scrutinise and present it report in the next Parliament sitting.

So far, we had actually received confirmation of five virtual submissions. Two will be done today and three will take place tomorrow, and all will be aired live on our Walesi Platform.

We had received numerous written submissions from the public which is very good that people are actually showing their interest when it comes to showing interest in Parliamentary work, especially when it is for the submission of such a Bill before this Committee.

Without further delay, we have before us, Mr. Peter Rigamoto, Head of Legal, Digicel Pacific Group. I now invite Mr. Rigamoto to provide the submission from Digicel and please note that if there are any questions fromHonourable Members of the Committee, they will interject or we will wait till the end of the presentation to ask all questions.

You can now introduce your good self and start with your submission, *vinaka*.

MR. P. RIGAMATO.- Thanks indeed to the Standing Committee on Justice, Law and Human Rights. Mr. Chairman, the Deputy Chairperson and Honourable Members as well as the Parliamentary secretariat and administration; we very much appreciate this opportunity to present our views on the current body of the Bill.

We are keeping our submission to three or four main points. There are many other points to cover but we believe those are the most salient points for the purposes of service providers.

My name is Peter Rigamoto. I have been working at Digicel for 10 years in the Legal Division. I am currently Head of Legal across our five Pacific markets, not including Papua New Guinea (PNG), but the other five markets that we take care of around the South Pacific.

We do hope our submissions are useful and before diving into the submission proper, we just wish to state that we support the ambit on cybersecurity and protection of national security and have assisted in the discussions on cybersecurity for a number of years now.

We have presented the Honourable Members of the Standing Committee with a written submission. We also have a somewhat summarised version in our presentation. If you will allow, it may assist in understanding our submissions quicker and we also wish to provide a brief on the technology used.

MR. CHAIRMAN.- Sure, Mr. Rigamoto, you can do that.

MR. P. RIGAMOTO.- I appreciate that, Sir. Please, confirm if you can see the presentation, Sir.

MR. CHAIRMAN.- Yes.

MR. P. RIGAMOTO.- The structure of our presentation today, Honourable Chairman, is, we will begin with a bit of technology context, then through to the hindrances on how some forms of technology might hinder the effectiveness of the legislation and then we will move in to our submission that has three main points.

If I may, Honourable Chairman, the first slide is a breakdown of internet utilisation in Fiji presented by Telecom Fiji Limited (TFL) through a conference paper some months ago, but it clearly shows that internet usage has increased more than 400 percent in the last five years.

MR. CHAIRMAN.- Mr. Rigamoto, if I may interrupt, I still cannotsee the slide at this point in time. I can only see the cover page or the first slide is not moving.

MR. P. RIGAMOTO.- Sir, let me attempt to resolve the technical difficulty. Please, let me know if you are able to see the next slide now?

MR. I. KOMAISAVAI.- Honourable Chairman, if I may interrupt, Sir.

MR. CHAIRMAN.- Yes, Ira.

MR. I. KOMAISAVAI.- I have the slide open from my end as well.

MR. P. RIGAMOTO.- Sir, this was the structure which I had spoken briefly about.

MR. CHAIRMAN.- Mr. Rigamoto, there is still some technical glitch. What we can do is, we can ask Ira if he can share the live instead.

MR. I. KOMAISAVAI.- Sir, the slides are with me, we do not really have to share the slides, Sir. For the purpose of the meeting, we can just let Mr. Rigamoto read from his submission. I can read the slides from my end without sharing it.

MR. CHAIRMAN.- Alright, can you just email the slides to me and to the Honourable Members?

MR. I. KOMAISAVAI.- Yes, thank you.

MR. CHAIRMAN.- Mr. Rigamoto, you may just read it out.

MR. P. RIGAMOTO.- No issue at all, Sir. I appreciate it.

Mr. Chairman and Honourable Members, the provision I wanted to take you through is more along the lines of what you see when you look at the internet technology. What you generally see is the app on your phone. You see windows on your computers, but what you do not see is that, behind is the network of interconnected computers throughout the South Pacific and the world.

Fiji, in particular, is connected by both, satellite and international fibre from FINTEL, and that is then transported through fibre and telecommunication towers to operators and then on to customers. Unfortunately, some of the hindrances in the way, which you will see in my slides also, some of the hindrances that may be found when attempting to implement this legislation is with respect to messaging Apps and also VPN and encryption. I will go into a bit more detail in the slides but let me see if I can, at least, share it in this form.

Messaging Apps such as *WhatsApp*, *Viber*, et cetera, have an end-to-end encryptions. What this means is, even if we were able to intercept it locally without the applicable key to unlock the encryption,

you will not be able to see what is behind the message. So, even if you are able to pull back the curtain, you will not be able to see beyond the code of our zeros and ones and other data points.

This is also the case with other technologies, such as VPN, so the Virtual Private Network which you can use to pretend that you are logging in from the United States if you wanted to watch the United States version of *Netflix*, for instance. So, there are certain software distractions in place where even if we were able to implement technology locally to look beyond or look into a person's internet connection, it will still be encrypted.

Moving on to Digicel's submission proper, in our written submission, we have said that the definition of 'service provider' was a bit too wide in one aspect but in the other was narrow. What we had meant by this was, subsection (d) which you might see on your screen at the moment but if you do not, the particular area of the definition of 'service provider' that we had issue with was having included, "an entity that processes or stores computer data". So, with that wide definition, quite a few non-service providers in the traditional sense, such as banks or even your ICT IP Parliamentary complex might be taken into that definition because you still process or store computer data.

So, our submission with respect to subsection (b) was potentially to narrow that aspect or say that it only applies to those service providers that provide services to the public. Therefore, it attaches to companies like our Digicel, TFL and Vodafone, but not inadvertently capturing small scale private SMEs or the IT divisions of different corporations, Government and NGOs.

MR. CHAIRMAN.- Mr. Rigamoto, I will have to interrupt you again. I am getting message from Parliament that the slideshows are causing interference in our live telecast. So, unfortunately we will have to go out of the slideshows, it is causing some technical glitches in our live broadcast.

MR. P. RIGAMOTO.- No issue at all Sir, it is appreciated Honourable Chairman.

MR. CHAIRMAN.- Apologies about that.

MR. P. RIGAMOTO.- No issue at all, Mr. Chairman. We are more than happy to continue and you have the slides and our submissions, so I will speak on them. It might not be as entertaining just listening to myself, as opposed to watching those slides but please, by all means, if you have any questions regarding the slides later, feel free to contact me and I will be more than happy to provide further information to the Standing Committee and if Mr. Chairman may require.

MR. CHAIRMAN.- Thank you. Yes, Mr. Rigamoto, you may continue.

MR. P. RIGAMOTO.- Thank you, Mr. Chairman. The first part of our submission was in respect to the definition of 'service provider'. In that, it was quite wide in subsection (b) in order to catch small scale SMEs and IT divisions of various corporations, so that was too wide.

But, at the same time, we believe that we as a service provider should, of course, be added. So what we have proposed is to amend the definition to include those who provide services to the public and thereafter, Mr. Chairman. That is, to also include, "those parties that provide digital platforms, such as social media content, communications and content aggregation functions." The purpose for this, Mr.

Chairman, is to ensure that those who must provide encryption keys to enable the viewing of data, are also covered under this legislation.

Mr. Chairman, moving on to the second part of our three-part submission, there was some provision in the legislation which required a judge or magistrate to provide its approval. Other provisions, such as seizure required the magistrate or judge, but there were other provisions which did not require it. And our broad submission is that, that should be required for various matters.

Also the threshold for serious offence was quite low in the legislation at six months or a fine of $500. Our submission is that the serious offence definition be bolstered to five years and a fine of more than $10,000.

MR. CHAIRMAN.- Mr. Rigamoto, can you tell me which clause are you talking about in the Bill itself?

MR. RIGAMOTO.- Yes, Mr. Chairman. For example, if we look into Clause 19 which is Expedited Preservation or Clause 18 of the current Draft Bill, so Clause 18(1) says, and I quote:

> "A police officer or authorised person may issue a written notice to a person to preserve specified data…"

The request for both of those do not require a judge or magistrate, but it is only required in Clause 19(2), to extend the term for such an application.

MR. CHAIRMAN.-So, the first 90 days is by the police officer?

MR. RIGAMOTO.- That will be correct, Sir.

MR. CHAIRMAN.- So, if it has to be more than 90 days, it has to go to the magistrate court or the magistrate.

MR. P. RIGAMOTO.- Yes, Mr. Chairman.

MR. CHAIRMAN.- So, what are you trying to say? Even the first 90 days should be on the basis that a magistrate or judge ordered, or what?

MR. P. RIGAMOTO.- That is for consistency sake, Honourable Chairman. Our submission is that, a judge or magistrate should preside over orders or requirements. And also to note that in the current search warrant provisions in legislation, they have a Justice of the Peace or a Magistrate. In this Cybercrime Bill, it is a judge or magistrate, but we believe that is a stronger threshold so we do not have a particular issue with that.

MR. CHAIRMAN.- So, what about the first 90 days? I am just trying to get it clear on where you are coming from.

MR. P. RIGAMOTO.- If there is a need for an order, our general submission is that, it should go before a magistrate or judge, at least, a magistrate in order to give effect to the court order.

MR. CHAIRMAN.- With regards to this, for example, if we need to actually preserve the data of a stored computer, let us say, in the pre-investigation of the police, how would they be able to go to the magistrate first before doing the investigation in order to obtain that data?

MR. P. RIGAMOTO.- The current status quo, even without the present search warrants, Honourable Chairman, is, if it is obtained quite quickly by the police, again, the mechanism is also through the Justice of the Peace which may be part of the reason why it is so swift. But search warrants and other warrants and orders are presently quite speedy being expedited but all we are noting is that, there are some…..(inaudible)…..

MR. CHAIRMAN.- So, basically what you are trying to say is, for example, a police officer needs to have a search warrant or something in order to actually enter the office to obtain the data. It is not just any officer can walk in into a particular office and obtain the data without any search warrant or anything from the higher authorities.

MR. P. RIGAMOTO.- Yes, Sir. The search and seizure is already under a different power, so that is under Clause 16 and that requires a judge or magistrate. While all our submission was … (inaudible)… in terms of matters which require a magistrate or a judge.

MR. CHAIRMAN.- Alright, that provides clarity, yes. Thank you. We can move on now.

MR. P. RIGAMOTO.- Thank you, Mr. Chairman.

The other information that we have brought to the fore in both, our submission and our presentation is the implementation issues with respect to Clauses 22 and 23.

MR. CHAIRMAN.- Just let me go to Clause 22 and 23, please. Yes, real time collection of data.

MR. P. RIGAMOTO.- Clauses 22 and 23 are obligations on service providers, which is fine. Again, with reference to our earlier point about the definition of service provider, it is currently quite wide. But if it was only Digicel, TFL, Vodafone and key providers for instance, there is a provision there that states that the Minister may determine implementation capacity, and that is in Clause 23(6).

(Inaudible)

MR. CHAIRMAN.- Yes.

MR. P. RIGAMOTO.- In our submission, Mr. Chairman, there is already a requirement for this assistance under section 74 of the Telecommunication Act 2008.

The original Budapest Convention to which this current Bill relates states that the party shall adopt the legislation to compel the service provider within its existing technical capability. So in short, Mr. Chairman, the Budapest Convention towards this has a requirement only up to existing technical capability, and the Telecommunication Act 2008 allows for a process of discussion before such measures are implemented.

We have made submissions as to what we would respectfully believe might be amendments for the purposes of your review in our written submissions. But broadly those provisions in the current Bill are higher than the Budapest Convention requirement but they are also already captured in the Telecommunications Act 2008.

So it is our respectful submission that those requirements of Clause 23(6), (7) and (8) and also Clause 22(5) and (6) are being dealt with under the current provisions of the Telecommunication Act 2008 through ongoing dialogue.

We especially make those submissions because of the fact that, even if a telecommunications operator, such as ourselves or TFL or Vodafone was forced to implement technology without all key providers also providing decryption algorithms, we still might not be able to see beyond. We could draw the curtain, but we could not decide what is at the back of the curtain.

So our respectful submission on that point, Mr. Chairman, is that this be taken back into the ambits of the Telecommunications Act 2008 for further discussion as to how we can do this properly in a way that achieves the goals of the Cybercrime Bill.

MR. CHAIRMAN.- Just confirming, Mr. Rigamoto, for Clause 23, is it Subclauses 6, 7 and 8?

MR. P. RIGAMOTO.- Yes, Mr. Chairman.

MR. CHAIRMAN.- For Clause 22, is it Subclauses 5 and 6?

MR. P. RIGAMOTO.- Yes, Mr. Chairman. Clause 23(8), I believe, is all right but it is really Clause 23(6) and (7).

MR. CHAIRMAN.- Thank you.

MR. P. RIGAMOTO.- Mr. Chairman and Honourable Members of the Standing Committee, that is broadly our submission. My apology for not being able to provide our print also, to assist us through.

However, to sum up, our view on the definition of service provider is that, it is currently too broaden and it even captures private SMEs, banks, et cetera. But we believe that can be amended by a small addition of those who provide services to the public, and then it will only catch "provider services" ourselves.

Thereafter, the other area which we have made written submissions on and added into our recommendations, that all key providers may also be bound by this legislation in the country.

And our other two provisions were the requirements for seizure and that discussion around the good and best Convention requirements in the Telecommunications Act with respect to Clauses 22 and 23.

MR. CHAIRMAN.- Mr. Rigamoto, just with regard to the definition of "service provider", what would be an active implication if we actually go with the current definition and incorporate all those

private entities, as you have mentioned, to be part of the service provider. What implications of that in the Bill?

MR. P. RIGAMOTO.- The only implication there would be Subclause (b) of that provision. So, I think the definition of service provider which is numbered Page 4, second definition from the bottom. When you go to Subclause (b), it says: "any other entity that processes or stores computer data."

When you say processes or stores computer data on behalf of the entity or users, so processes or stores, for example, in the Parliament of Fiji is your IT Division of the Secretariat will have to process or store some of your data. So, they are inadvertently caught.

Our submission is, at the end of this Subclause (b), to specifically add that this is only for providers of services to the public. So, by narrowing it down to "providers of services to the public", it only captures providers such as ourselves.

MR. CHAIRMAN.- Alright, I do understand the context that you are coming from, but my question is, for example, if I own a private company App and we are actually doing networking between my 10 or 20 branches, but we do not actually store our own data. We have someone …… (inaudible)…. which is not a telecommunications company but just a company that is providing a server which we actually hire to store data. How are we going to capture that if you are going to amend this particular provision in the Bill?

MR. P. RIGAMOTO.- The key areas that utilise the definition of "service provider" is mostly around those two Clauses we talked about, Clause 22 and Clause 23. The other provisions of e seizure and the rest, they can be implemented on any person. So, that even includes those types of people that we talked about who might host externally. But the service provider requirements are strictly with respect to Clauses 22 and 23 which are about interception and traffic records which is more in line with what we provide as a service. But it does not stop seizure of data.

MR. CHAIRMAN.- Thank you, Mr. Rigamoto, for that clarification and that is actually well-taken on board. We have noted it down. So, once we do our Committee deliberation, we will have some more deliberation on that aspect of the Bill. Mr. Rigamoto, anything else from your side?

MR. P. RIGAMOTO.- Mr. Chairman, I have nothing further. I believe the only other question I would have will be on the process. I recall that the Cybercrime Bill first came into consultation in 2015 approximately, and then I know it was a Bill in 2019 and then a Bill brought back to the Standing Committee today. What would be the next steps along the journey for this Bill?

MR. CHAIRMAN.- What will happen now is since the Bill is before Parliament and Parliament has passed the Bill to the Committee, the Committee is now doing its independent inquiry. Once we have collected all the submissions, we will sit and then review what needs to be done with regards to the Bill. Then we will refer the amended Bill back to Parliament. It will be debated upon and if passed, it will be gazetted as an Act.

MR. P. RIGAMOTO.- I have nothing further, if you have nothing further for me, Sir.

MR. CHAIRMAN.- Honourable Sharma and Honourable Dr. Govind, do you have any further clarification or opinion to be made to Mr. Rigamoto?

HON. DR. S.R. GOVIND.- Mr Chairman, I do not have any further comments, thank you.

HON. R.R. SHARMA.- Thank you, Mr. Chairman. At the moment, I do not have any comments and only if I can look over the copy of it and then come back to it again.

MR. CHAIRMAN. – Thank you, Mr. Rigamoto.

On behalf of Standing Committee on Justice, Law and Human Rights, I would like to thank you for your time in coming forward to present your submission. We request if you can email us your presentation, we will go through it and if there is any question, the Secretariat will get back to you on that. Thank you very much.

The Committee adjourned at 9.57 a.m.

The Committee resumed at 10.37 a.m.

Online Interviewee/Submittee: **Office of the United Nations High Commissioner for Human Rights (OHCHR)**
UN Office on Drugs and Crime (UNODC)

In Attendance:

(1)	Mr. Thomas Hunecke	-	Acting Regional Representative for the Pacific, OHCHR.
(2)	Ms. Releshni Karan	-	Legal Advisor, OHCHR.
(3)	Mr. Alexandru Caciuloiu	-	Cybercrime and Cryptocurrency Programme Coordinator – South East Asia and the Pacific, UNODC

MR. CHAIRMAN.- Welcome back, Honourable Members, and our viewers. A very special welcome to our submittees from the Office of the High Commissioner for Human Rights Commission (OHCHR) and UN Office on Drugs and Crime (UNODC). Our second submission is a joint submission from the two UN Offices mentioned above. Before us, we have Ms. Karan, Mr. Hunecke and Mr. Caciuloiu.

We, as a Committee, are very grateful with the help provided to us by OHCHR in securing an expert to discuss the Cybercrime Bill. As everyone is aware that the Cybercrime Bill has been presented and read through by the Honourable Attorney-General under Standing Order 51, so the Bill has been referred to the Standing Committee on Justice, Law and Human Rights and we are law-binded to scrutinise this Bill in the next 30 days and present a report back to Parliament for its second reading.

For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are open to the public. Please, note that this is a public hearing and is open to the general public and media, and it is also being aired live on our television in the Parliament Channel on the Walesi platform and Parliament website.

For any sensitive information concerning this inquiry that cannot be disclosed in public, this can be provided to the Committee, either in private or in writing. However, please, be advised that pursuant to Standing Orders 111, there are only few specific circumstances that allow for non-disclosure of this, which include:

- national security measures;
- third party confidential information;
- personnel or human resources matters; and
- deliberation and development of Committee reports and recommendations.

At the outset, I wish to remind Honourable Members and our witness that all questions are to be directed through the Chair. This is a Parliamentary inquiry and all information gathered is covered under the Parliamentary Powers and Privileges Act.

In terms of the protocol of this Committee hearing, please be advised that there will be no usage of mobile phones and all mobile phones are to be on silent mode while the meeting is in progress. Now, I would like to introduce the Honourable Members of the Committee.

(Introduction of Honourable Members)

Thank you, Honourable Members, for introducing yourselves. Before we hand over the floor to our submittees today, just a quick reminder, if there are any questions in between, we shall interrupt to ask those questions or we shall preserve those questions till the end when we may interject and ask those questions for further clarification.

I now hand over to our submittees if they can introduce themselves and then we can go into the submission proper.

MR. T. HUNECKE.- Thank you Honourable Chairman. You had already kindly introduced the members of the joint UN Team, so my name is Thomas Hunecke. I am the Acting Regional Representative of the Pacific, Office of the United Nations High Commissioner for Human Rights and I am joined by Ms. Releshni Karan, who is our Legal Advisor. It gives me great pleasure to also quickly introduce Alexandru Caciuloiu, who is the Cybercrime and Cryptocurrency Advisor at the Regional Office for South East Asia and the Pacific at the United Nations Office of Drugs and Crime (UNODC) based in Bangkok.

Honourable Chairman and Honourable Members of the Committee, it is a privilege to address you again and we have come before back in 2019. The role since completely changed, but let me just say that the work at OHCHR should be an elementary part of our work to provide the Standing Committee with advice from human rights perspective and today, we can do that in the form of a joint submission with UNODC which is of great importance.

For us, it is a first call that we have two agencies who make a joint submission which, from our perspective, increases the value even further but that is an important point so that you have a joint submission by two UN agencies.

Let me touch up on the actual submission. Of course, I forgot, I hope that you and your families are all doing well, given the current circumstances that the world finds itself.

Let me speak about the actual joint submission. The OHCHR and UNODC, we very much welcome the opportunity to provide comments and technical guidance on the Bill through this written submission that we have made. And, of course, we stand ready to provide further advice to the Standing Committee as you deemed necessary.

The Bill has been analysed, taking guiding principles and best practices into consideration and is generally found to be well-structured. Our joint submission focuses on making suggestions and comments to address existing gaps in the legislation as related to computer crimes; recommendations geared towards improving the current text of the Bill; and, offering *de lege ferende* proposals for purposes of coherence, consistency and comprehensiveness of the legislative framework.

Honourable Chairman and Honourable Members of the Standing Committee, our joint submission also highlights some concerns arising from the Bill from an international human rights Law perspective. I would like now to give the floor to Ms. Karan and to Mr. Caciuloiu. Over to you colleagues, please.

MS. R. KARAN.- Mr. Chairman and Honourable Members of the Committee, please, allow me to take you through the submission. We have filed this written submission and it is quite detailed and spans over 16 pages. So I will not take you through each and every provision that is stated there, I will just take you through the key points and the things that we wish to highlight.

We will start with the fact that participation be welcomed. The fact that this Bill is currently undergoing a meaningful, sort of, consultative process where you are inviting all the relevant offices to come and make submissions before you, and will file a report for the next second reading. That is very much welcomed, given that there are several restrictions in place in Fiji due to the COVID-19 pandemic and it makes participation a bit of a challenge.

So, we really appreciate that from our side and we encourage you to also continue holding nationwide consultations and ensure that all groups in society are properly represented and can participate in this process and not just the key organisations as it is quite applicable to everyone in Fiji, especially those who are marginalised or discriminated against, including women's groups.

The use of ICT in this, sort of, nationwide consultations are normally used in this very challenging times. We have on page 3 of our submission, asked that the use of ICT and what measures are needed to be undertaken can be found in the guidelines for States for effective implementation of the right to participate in public affairs. You could get a lot of measures, a lot of safeguards that is there and, sort of, implement it and that will help in this participation.

We have done a thorough analysis of the national legislation and we feel that this proposed legislation will have to be harmonised with the existing legislation. Some of the legislations that this particular Bill has to be harmonised with are the:

- Online Safety Act 2018;
- Crimes Act 2009;
- Telecommunications Act 2008;
- Copyright Act 1999;
- Income Tax Film Making and Audio Visual Incentives Act 2015; and
- Proceeds of Crimes Act 1997, just to mention some.

This is not a comprehensive or an exhaustive list, but this does give an indication that there are several laws that affect computer-related crimes and will have an implication. So, what we are basically saying is that, all these laws must be harmonised so that there is consistency between the laws. As some may have a higher degree of criminal sanctions, whereas some may have a lower degree of criminal sanctions. So, it is good to harmonise that at the outset.

Both, UNODC and OHCHR are ready to provide guidance on this to the Government of Fiji should our technical assistance be necessary because apart from legislation, there is a need for law

enforcement agencies to be provided with the necessary tools to investigate cybercrimes, and these are sophisticated tools and quite different from what is used by the law enforcement agencies.

Taking you through the Cybercrime Bill 2020, it is divided into seven Parts. Part 1 contains provisions - the usual preliminaries that include interpretation and jurisdiction.

Part 2 refers to offences that relate to confidentiality, integrity and availability of data and computer systems.

Part 3 features computer-related and content-related offences.

Part 4 contains provisions dealing with other offences, such as identify theft, theft of communication services and disclosure during an investigation and failure to provide assistance.

Part 5 outlines the procedural measures that need to be taken by law enforcement agencies and authorised persons.

Part 6 includes provisions for international corporations.

Part 7 contains provisions on the related regulations that may come up.

There is a lot of guidance material that is available online and there is a lot of advisory material that the UN has produced. We have listed on page 4 of our submission, some of these advisory materials that the Committee should look at to align the legislation to international standards. This is, again, not an exhaustive list but we recommend that you look at these international instruments to fine-tune on issues of our grey areas that may need work.

Going into the legislation proper now, the word "cybercrime" has been used throughout the text, in a number of places including its headings and subheadings. For clarity, we feel that the term "cybercrime", must be properly defined and it should be specified.

Cybercrime has a different meaning to computer-related crime and it has a different meaning to network crimes, so the definition of that, how the Fiji Government sees it, needs to be compressed and specified in the interpretation section.

Another term that is used throughout this Bill is the, "reasonable excuse." It should be well established, either in case or statutory law. If not, an overly broad interpretation of the concept can lead to over criminalisation and human rights violations. We are not saying that there will be human rights violations but it is so open that the term can be used in that context that violations can occur, if it is not used properly.

The Bill should be amended to delete potentially ambiguous terms such as, "reasonable excuse". It is recommended that there should be specific terms or specificity of the offences included, with expressed requirement that the conduct involved is done "without right." The term "without right" needs to be used instead.

The recommended term "without right", reflects the insight that the conduct that is described is not always punishable *per se*, but it may be legal or justified in a few instances, where legal defenses are applicable. For example, in some places where consent may be given, self-defence, necessity or where public interest leads to exclusion of criminal liability, those will be covered if we use the term "without right".

The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement their concept. For example, there may be a court order that allows them to do this, there may be a legislation order given or an order from an executive that allows them to do this, or it may be just consensual between the supervisor and the person. So all these are very excusable legal defenses and justifications, and international principles should be embodied, which is why we are saying that that terminology that is used in this legislation should be looked at again and the general crux of it. So, "reasonable excuse" should be amended to say, "without right". That is our second submission.

There are certain provisions which are not included in this Bill which we feel should be included. The provisions on the misuse of devices, is not included in this Bill. This is quite important because such provisions are also consistent with Article 6 of the Budapest Convention, which is one of the guiding documents and it relates to the sources of offences.

(Inaudible)

I apologise, I think we got cut off there. So, just going on with that, the provisions that relate to the misuse of devices, are established as separate and independent criminal offences as part of the Bill. This is because we are in the dark side of the computer crimes, you will see that issues, for example, there are hacker tools, there are things that hackers use to ensure that they are able to conduct these criminal issues online or using computers.

So, if you put "misuse of devices" in the Bill, you will in effect prevent something which is called a black market for these hacker tools to be produced or distributed. So, this is a very important provision which we are submitting, should be included in the Bill. You must misuse those devices and tools that hackers, crackers and all the others use to do potential dangerous acts online.

Furthermore, we also see a need for the Government to address hate speech and online content that incite racial or religious hatred, that constitute incitement to discrimination, hostility and violence. We are of the opinion that the acts of racism or xenophobic nature constitute a violation of human rights and the threat to the rule of law and democratic stability.

As you all know, Honourable Members, the internet is used quite frequently in Fiji to incite racial hatred and target certain groups. It is very important that now, you have the Cybercrime Bill to address those issues and we believe that this legislation can provide adequate legal responses to the propaganda of a racist or xenophobic nature that is committed through computer systems.

The additional protocol to the Convention on Cybercrime concerning criminalisation of acts of racist or xenophobic nature can provide guidance on this. We have included that in the list of guiding documents, should you wish to have a look.

The drafters of the Bill have continuously in their explanatory note, referred to the Budapest Convention so this Protocol is part of that Convention. It is an additional protocol to the Budapest Convention.

We believe that you must look at it holistically, if you are applying this Convention and the United Nations Special Rapporteur on the Promotion and Protection of the right to Freedom of Opinion and Expression has actually said that forms of expression should be prohibited by international law, amongst them advocacy of national, racial and religious hatred that constitute incitement to discrimination, hostility and violence and direct or public incitement to commit genocide. The social media and computers, they all play a very strong role in inciting racial violence or racial hatred. So, this can be addressed through this Bill.

Going further, we submit that the provisions of the Bill should afford the same rights and limitations consistently to persons online, as it does to people who are not online or not using computers. So, it should be consistent.

The United Nations Human Rights Council has repeatedly affirmed that the same rights that people have offline must be protected online. So, freedom of expression, freedom of assembly, so all of those needs to be protected. The right to education, the right to cultural life, all of that needs to be protected.

Clauses 1 and 2 of Part 1 are very much consistent with the Budapest Convention so I will skip that.

Part 2 of the Bill basically looks at the applicability of the Bill. We would like the drafters to perhaps, review this portion to ensure that there is no overbroad or excessive jurisdiction. At this stage, the provision does not require physical location of the affected computer systems or data in Fiji. So the world is your oyster, the crime can happen anywhere. Your national can sit anywhere in the world, so all those things need to be perhaps, reconsidered again. But in terms of the nationality, if extradition is not possible, yes, that is consistent.

Clause 4 in Part 2, the only thing I would like to say on this is that the idea is to improve the means to prevent and supress computer-related crime by establishing a common minimum standard. Right now, there are different laws providing different sanctions. There has to be a common minimum standard for offences across Fiji. It does not matter whether you are going through the Online Safety Act or through the Cybercrime Act, the sanction needs to be, sort of, equivalent and it needs to be consistent. That sort of harmonisation is needed at the national level.

Mr. Chairman in Clause 5 - Part 2, this provision needs clarity because it is not clear whether the offences in question is the unauthorised access to a computer system or computer data. The mere unauthorised intrusion - hacking, cracking and computer trespass should, in principle, be illegal. However, it will lead to impediments of legitimate users, so you got to have those safeguards.

The term “access” needs to be properly defined and we have gone through lengths in our submission to properly define it for the Committee’s consideration.

There should not be criminalisation…

MR. CHAIRMAN.- Ms. Karan, apology to interrupt. What do you actually mean when you say 'legitimate users', would you be able to give an example to that? Actually, what would be the legitimate ones?

MS. R. KARAN.- For example, testing this device. You have a group and every organisation in Fiji, sort of, has a section that looks after its testing, its authorisation, there would be persons who are authorised to use that particular programme or a particular data amongst a certain group of people, so that is rightful use.

Actually, the term that you can use for access is 'with right' or 'persons without right'. Those terms can fix the ambiguity in this provision. I apologise if I am going through more legal sort of thing, that is not my intention, but it is just a suggestion that those terms are what is considered as proper terms. Even in the Budapest Convention, they are recommending that States use these terms to prevent ambiguity, so we are, sort of, putting that across.

If Honourable Committee Members see fit, we can share the explanatory note to the Budapest Convention, so you get a much more exhaustive way to deal with these issues. We could share it, if you so wish.

MR. CHAIRMAN.- Yes, we welcome that idea, Ms. Karan, if you can actually share those information with us so that we have a better understanding with regards to the Bill itself. It is because how we actually take it, I believe is like, for example, if I have something to be done in my network or my device owned by me or my company or anyone for that matter, if they are given authority, that is it. It becomes a legitimate interference into the network itself but if they do not have, even my network provider tries to enter into my network without my knowledge, so that becomes illegitimate.

MS. R. KARAN.- Yes, but there has to be clarity in the wordings of this provision.

On a pure legal basis, it seems that it very unclear because the Bill defines the computer data differently from computer system and differently from computer network. So those terminologies have to be very well looked at when you are actually dealing with this provision because even though you are looking at it holistically, when you apply this in Court, those will become justifications and defenses, as well as it will be ground for movement and discretion. So to prevent that, we are highlighting that there is this gap in the usage of the terms.

Clause 6 - Part 2, this section aims to protect the right of privacy of data communication. The right to privacy, of course, is enshrined in the Constitution of Fiji and this principle has to be applied to all forms of data, electronic data, by telephone, your fax, your email and your file transfer.

The offence represents the same violation of privacy or communications as traditional tapping or recording of your conversations between persons. What we are trying to say is that, the provisions needs to be consistent to other legislation that protects communications services by criminalising the illegal interception of phone conversations. You may want to look at the telephone, the Telecommunications Act or what the Military uses or what the law enforcement uses, because in this provision there is no exceptions, there is no limitations.

Exceptions, for example, law enforcement authorities, whose surveillance is necessary in the interest of national security, or for detection of offences by investigating authorities, those are not covered. So, how will this work? Those things need to be sort of relooked at and in a way that it will be defined so that it consistent and it does not, sort of, be contradictory to the other legislation.

Clause 9 - Part 3, in this section the provision has words, again, it is a terminology thing. Words, such as 'loss', 'gain', et cetera. What does this mean? Does this mean a financial gain or a financial loss? Does it mean a risk of loss? Does it mean damage to reputation? What does the loss mean? Does it mean financial or does it mean reputational? You know, how you are defining it. So, those sort of things need to be very, very precise when you are making this legislation because then, you will open up the entire Pandora's box and you will get a lot of things coming up. For example, I had loss of sleep. My reputation suffered, and things like that. So, it is the terminology thing that we have to do.

We recommend that you consider the wordings and take queue from Article 7 of the Budapest Convention of what 'loss' or 'gain' can be substituted with, and we have provided that in the written submissions for your easy knowledge and access.

Clause 10 - Part 3, basically the elements of the offence as described in this Part in relation to the conduct of computer-related extortion is quite evident and it is alright. But is it not alright in the case of computer-related fraud.

The reason why I am saying this is because in Fiji, there are market regulators. They regulate the market, for example, commercial practices with respect to market competition can cause an economic detriment to a person, or benefit one person but not necessarily benefit the other.

They are not usually carried out with fraudulent or dishonest intent in all cases but those should not be, sort of, criminalised, it should be allowed. So, the offence must be committed without right. Again, we are asking that you consider using this terminology which is 'without right' here because that will cover the economic benefit that would be obtained without right.

Of course, there is legitimate commercial practices which are intended to procure economic benefit, they are not meant to be included in the offence. So, those things should be an exception.

Clause 11 - Part 3, I would like to go through this Part quite extensively with the Honourable Members because it is very important.

From an international standpoint of view, the term 'child sexual abuse material' is increasingly used to replace 'child pornography'. In the international world, we no longer used this term 'child pornography', we use 'child sexual abuse material.

So, the switch of terminology is, sort of, based on the argument that sexualised material that depicts or otherwise represents children is, indeed, a representation and a form of child sexual abuse. It should not be describe as pornography because the term 'pornography' is used primarily for adults that engage in consensual sexual acts that are distributed to the general public for their sexual pleasure. So, the terminology here we are, sort of, respectfully submitting that you consider to change that terminology from 'child pornography' to 'child sexual abuse material'.

Furthermore, we are against this term 'child pornography' because we feel that this act, sort of, denotes that it is carried out with the consent of the child, and it represents legitimate sexual material. We are saying that this term 'child pornography' is overly broad and it needs clarification.

Now, the reason also is because it will make prosecution and policing of this law very, very difficult. It may be useful to suggest that the language be added to the legislation to further explain what this term means, if you want to still use term 'child pornography', but you will have to further define this term, because as it stands, it is not properly clear.

In addition, it is not clear how it will be determined that the image of video is that of a child. How can you know that the video you are watching is actually even a child? It may be a grown up woman that looks like a child, so there is policing issues around this.

Similar to the issue that I have just highlighted, there needs to be a description to clarify what exactly is illegal. For example, you might want to cap it by age, and how will you determine that? So, it is recommended, again, that you use the term 'without right' in these provisions, as it does not exclude legal defenses. And, yes, they are legal defenses to this as well, where for example, a party …. (inaudible)…

MR. I. KOMAISAVAI.- Honourable Chairman, it seems the video feed from Ms. Karan has stopped. She was reading through the submission that was sent.

MR. CHAIRMAN.- We will just wait for a while for her to come back on again.

MR. I. KOMAISAVAI.- Sir, I think she is coming back on from the video from Mr. Hunecke.

MS. R. KARAN.- I apologise, I think something has gone wrong in my computer.

MR. CHAIRMAN.- That is fine.

MR. A. CACIULOIU.- You are muted, Ms. Karan.

MR. I. KOMAISAVAI.- Ms. Karan, your microphone is muted.

MS. R. KARAN.- My apologies, thank you. For your indulgence, I do not know what is wrong with my computer. Thank you, Mr. Hunecke, for allowing the use of your computer.

What we were basically saying that the policing of the child pornography entire sections will be very difficult. It has to be done without right to allow for legal defenses, such as to take into account fundamental rights like freedom of thought, expression, education and privacy.

Basically, pornographic material is sometimes used in medical field. It is used in scientific field, it is used in artistic nature or in drama, or different sorts of things. All those things should still be allowed, it should not be that there be a blanket cap that there should not be any explicit material that is to do with children. It will curb all those other rights. There has to be allowances for legal defenses, and by the use of the term 'without right' you will, in effect, allow everyone to, sort of, be within that ambit.

A medical school can, for example, show a picture of a child explaining what it is without being classed in this, so those illegitimate defenses should be allowed.

There should be a section that should allow child abuse material to be uploaded to INTERPOL or child sexual abuse database. And as you know, Fiji is part of INTERPOL as well, so any specialised offices that work with their seized material, they can identify victims and ensure that the rights of the victims are also protected because sometimes you do not find the perpetrators, you find them five or six years down the lane and INTERPOL is quite useful in this area, so for better policing, those provisions should be added there.

MR. A. CACIULOIU.- If I can jump in, Ms. Karan, just for one second. I think what was important here is to highlight that, of course, child abuse material should be criminalised possession. Just a mere possession of child-abuse material has to be criminalised because this usually opens up the door for law enforcement operations, like this is how it usually it starts by being able to see who is sharing or uploading child abuse material online. Law enforcement can take a lead and just the mere fact that you are uploading or viewing this material is a crime.

This, nevertheless, has to allow for law enforcement to operate. So, usually when we arrest someone who possesses child abuse material, we take this material and we take it to a digital forensic lab, and we have specialised experts who work on these material to try to identify the victims in the videos or in the photos.

So, this is very complex work and they need to be able to link up these material to international databases, such as the INTERPOL Child Abuse database or the International Child Sexual Exploitation (ICSE) Database or the National Centre for Missing and Exploited Children (NCMEC) Database. So, that is why it is important to allow for some provisions so that law enforcement can work on these material to identify the children. Thank you, Mr. Chairman.

MR. CHAIRMAN.- I thank you. Just a clarification, when you are saying to upload child abuse material on to the database of INTERPOL, are you recommending that on request basis or any time you have data it should be uploaded?

MR. A. CACIULOIU.- I am not sure if Fiji, at the moment, is connected to the ICSE Database. This Database is available to all INTERPOL member States but not all of them are connected to the Database.

Once you are connected, you receive a training and you have some dedicated officers, whose fulltime job is to make sure that whatever seized television material throughout the country, it is uploaded to this Database. This also comes in with an obligation of the member State of Fiji to respond to requests from other countries.

Let us say, some child abuse material is found in a possession of a pedophile in a third country and then police worked on that material and they identified children that speak perhaps, a local language in Fiji. Then they will contact officers in Fiji and request them to look at the material and see if they identify maybe the location, if they find the setting to be from Fiji, so this is kind of once you join, you have certain obligations.

MR. CHAIRMAN.- Putting that into context, what you are saying is, for example, I will use the word 'pornography', a child pornography, is loaded on internet, are you saying that same pornography should be uploaded in the Database as well so that it can be identified in which country it is coming from, et cetera?

MR. A. CACIULOIU.- Mr. Chairman, what I am saying is, we are not uploading any material, it is the law enforcement. This is a material that has to be strictly controlled and any possession usually is penalised. So law enforcement is an exception to that because law enforcement needs to be able to work with these materials to identify these children to save them from harm.

We are not saying that these material should be allowed to be uploaded to any platform. So, the legislation just have to mention in very, kind of, drastic and not very over-specific terms, but to just allow law enforcement to work on these material, but this will not be uploaded to the internet, never! And this Database is strictly controlled and the characteristics of the materials that are uploaded are sanitised. So not the full child abuse material is uploaded, but only materials that allow for identification.

MR. CHAIRMAN.- All right, that is well noted.

MR. A. CACIULOIU.- The sanitised version of the material.

MR. CHAIRMAN.- So not the actual content?

MR. A. CACIULOIU.- Exactly!

MS. R. KARAN.- Mr. Chairman, if I may just add to what Mr. Caciuloiu said, the purpose of uploading these material to INTERPOL Database is to ensure to identify the victim, to provide support to them and to also ensure that they are not further victimised. This Database is extremely confidential. It only goes across one or two officers, who actually use this, even at the INTERPOL level.

Moving further, the lawmakers in Fiji should also consider criminalising other acts that involve protection of children online, while you are dealing with this particular provision.

We are respectfully submitting that offences like online grooming, lying to a child online in order to commit child sexual abuse and exploitation, harassment and prohibition of cyberbullying of children, all these should be criminalised under this legislation. Of course, it has to go through the proper drafting process and safeguards, again, in terms of the age of the children, identifying the victims and how the law enforcement will be done, but I think this is the exact legislation where it needs to be mentioned because right now, children in that sphere, it is a grey area on how we protect those children who are abused online.

Part 4, we recommend that the Government of Fiji also consider including ancillary liability of aiding, abetting and its related sanctions in the Bill to be included. Right now, it just refers to the offender and not actually someone who has aided and abetted. It can be two different people when it comes to computers. It can be a group, a whole network of people or whole network of computers. It does not even have to be people, it can even be computer to computer, or someone who is just an Internet Service Provider (ISP) provider.

That angle also needs to be looked at because here, when you are considering cybercrime, you are actually crossing the traditional borders. It does not have to be between people and people, it can be people and devices, devices to devices and you are not looking at geographical boundaries. Under this Part, there should be some clarification give on how we deal with someone who has assisted in that, ensuring that the material is disseminated.

Clause 17 – Part 5, I would like to just quickly go through these ones, not too much in detail, because I understand we have provided the submissions and it is quite comprehensive.

In Clause 17, it lists computers but does not include cell phones and tablets, for example, or other devices. There is no definition within the legislation that indicates that computer includes all of these terms, so in terms of our legislation which is the Cybercrime Bill, you need these definitions.

It is a terminology issue that you know, you have to have, sort of, clarification. There needs to be limits and procedures in place to limit the spread and redistribution of contrabands, like child exploitative files, for example.

Clause 18 contains a series of provisions for the authorisation of investigative powers that is used to gather electronic evidence. As highlighted in the thematic discussions internationally, an important factor that needs to be taken into account is the compliance with established procedures that safeguard human rights. So whichever, if your procedural measures are taken in terms of law enforcement, there has to be human rights mainstreamed in it in terms of investigative techniques that include the use of undercover agents, remote forensics, especially on the dark net.

It is vital for the drafters of national legislation to consider the issue of whether evidence obtained, for example, infiltration can be adduced in court, and if so, whether the undercover agent has to reveal his or her identity. It is important to balance the interest of justice with the need to ensure a fair trial to the accused. So, there has to be a balancing act when the drafters go in with this provision.

You have Article 20(1) of the United Nations Convention against Transnational Organised Crime. It does not require State parties to take such measures to allow for admissibility right now in court. From the use of special investigative techniques, this is an element which refers to positive obligation, to have laws and regulations in place for the sake of legal clarity and proper administration.

There is investigative techniques assessed that is allowable for the military and for the law enforcement officers when they are doing investigation. Perhaps, Mr. Caciuloui might like to add something on this aspect in terms of investigation and what they need to be, sort of, mindful of.

MR. A. CACIULOIU.- I think what this Part refers to is that, we need to be aware that there are certain special investigative measures that may infringe upon human rights of the citizens and we need to make sure that those special investigative measures only apply under certain cases and with the due provisions and checks and balances in place. Of course, it is up to the Committee and the Parliament to decide whether you want to accept these measures as evidence in court or not.

I believe that under certain crimes that are more severe, it is important to have a wide array of investigative measures in place, but those should only be allowed under certain conditions and with proper checks and balances with judicial authority and with all the full-fledged provisions.

MS. R. KARAN.- Keeping to Clause 25, it may be prudent to identify the competent authority that performs the functions described. In this provision, on behalf of Fiji is the Honourable Attorney-General, but there are privacy issues and there are also other issues of how these exchanges will take place, the safeguards.

The Minister for Communications, even though right now may be the Honourable Attorney-General but it has to be futuristic. This legislation needs to be futuristic as well, so the Minister for Communications should have that power to do all necessary under this legislation. It can be the Honourable Attorney-General but perhaps, there has to be more provisions on why there is a need for another person to come on board when you are dealing with this data because right now the data that you are dealing with has to go through only those hands that deal with it, such as the law enforcement agencies and those persons who are authorised to even see the data. Now, you are taking it out and giving it to another body altogether, then you have to justify that. So, those things need to be relooked at.

Clause 26 by virtue of this provision, the offences established in accordance with the Act are being extraditable offences. It is reminded that double criminality is a requirement for extradition from Fiji. And due to the specific nature of the offences under discussion, the relevance of section 3(2) of the Extradition Act may need to be reconfirmed.

Clause 28, the last section that we wish to submit on is that, this provision specifically provides for limitations on the use of information or material in order to enable the requested party in cases in which the information or material is considered particularly sensitive, to ensure that its used is limited to what the assistance is granted, and to ensure that it is not disseminated beyond law enforcement agencies, for example, it should not go to a political party. So, there has to be those safeguards in place. These restrictions provide safeguards which are available for data protection purposes.

It is not understood why the Attorney-General, as opposed to the Minister for Communications will receive this request only. And we recommend that due to issues of privacy, the information should rest with the line Minister.

That is just our recommendation. I will give the floor to my colleague, Mr. Caciuloiu, to wrap up this presentation. Thank you very much, Mr. Chairman and Honourable Members for listening to the submission so intently.

MR. CHAIRMAN.- Thank you, Ms. Karan. We shall now give the floor to Mr. Alexandru Caciuloiu for his contribution towards the submission. Thank you.

MR. A. CACULOIU.- Thank you, Ms. Karan. The extinguished Committee, I would like to start with a short intervention with cybercrime statistics.

According to a report published by cybersecurity ventures, cybercrime across the world, around $6 trillion annually by 2021. This is nearly six months from now. This has risen from around $3 trillion in 2015, so it is estimated that cybercrime will be more profitable than the global trade of all major illegal drugs combined.

This report also estimates that cybercrime damage caused could potentially double during the outbreak and this is not only due to fishing but also to an increase volume of ransom work action securing

more taxes to appropriate networks and employees exposing login credentials and confidential data to members at home.

We have seen also throughout the pandemic that there has been a steep increase in online child abuse as children are stuck at home being schooled online. This coupled with Fiji's increased connectivity and internet penetration within the population is bound to create risk. This is a stark reminder of what is looming ahead. I think that is why having proper cybercrime legislation in place is an essential step in making sure that Fiji will have what it takes to fight against this threat.

Therefore, I would like to congratulate this Committee for taking strong steps towards this direction and to highlight that the timing of this could not have been any better. I think it is important to understand that having a cybercrime law is a great first a step, but it is not the end of the journey.

If Fiji is to stay on top of the looming cybercrime threat, what needs to follow up as the cybercrime law is a comprehensive National Cyber Security Strategy that maps out all of the Government agencies and their responsibilities regarding the fight against cybercrime and towards a safe and secure cyber environment. Once these agencies and entities have been properly assigned the responsibilities, the Government may need to also make sure that they have the necessary tools and skills to deliver.

Therefore, next comes the strengthening of the criminal justice system in order to be able to properly enforce the new law. This means training the police, the prosecutors and the judges on the new law on how to handle cyber offences and on the ever-increasing amount of digital evidence that will be presented in the courts.

People need to be upskilled to adapt to the new legislation and they will need to get the necessary tools. And now let me tell you that those tools and skills do not come cheap. They take years to protect and they need constant updating and will require a recurring expense. This, unfortunately, is just the cost of doing business.

Cybercrime and digital forensics are both highly technical and highly specialised fields. Training takes time and is expensive, and the tools needed in this field are also updated every year in order to keep pace with the ever-evolving nature of technology.

Now, keeping these skills and tools updated is not the choice unfortunately, but it is a mandatory role that the Government needs to be fully aware of and Government needs to be able to allocate the proper resources so that your police officers, prosecutors and judges will have all the skills and the tools necessary to keep the country safe from cybercrimes.

Now, the good news is that, you are not in this alone. Both our agencies, the United Nations, are here to help. Throughout my activities with the UNODC, I have been supporting countries all over Asia and the Pacific by providing, not only legal support such as what we were doing now with our colleagues from OHCHR, but also delivering the necessary training, equipment and mentoring to the police, prosecutors and judges in order to strengthen their capacity to deal with all types of cyber offences.

I am happy to say that also I have been to Fiji in 2018, I was hoping to be able to be there live with you on this occasion as well, hopefully next time. In 2018, we conducted a regional Cybercrime

Long Table Discussion and we delivered an introductory training course on cybercrime. That was only a sample of what we can and are willing to do for Fiji moving forward.

Only last year, we have established a digital forensic laboratory in Laos and that entail providing a full instalment of tools, equipment, training and mentoring, so that the newly assigned officers can analyse digital evidence up to the latest international standards.

Now, we are here to help Fiji start on its journey and we are ready to be here all along the way, leading Fiji to becoming an important partner to the international community when it comes to the global fight against cybercrime.

In wrapping up my short intervention, I would like to inform the Honourable Committee about some of the latest UN level discussions on cybercrime.

During last year in the General Assembly, the Cybercrime Resolution pushed by Russia to require the United Nations Secretary-General to collect countries' views about cybercrime has passed and successfully placed discussions of a possible cybercrime treaty on the UN agenda.

Indeed, on 27th December last year, Russia moved forward once again with this latest resolution to establish a Committee of Experts to consider a new UN cybercrime treaty. This committee is to meet this August in New York to discuss the proposed convention. This is just to highlight that the issue of cybercrime is as present as ever on the international scene and, again, to highlight the timeliness of this Bill's introduction.

I would like to thank the Committee for allowing me to speak and I would like to reassure you that the United Nations is continuously committing to support Fiji on their journey to ensuring a safe and secure internet. Thank you.

MR. CHAIRMAN.- Thank you very much, Mr. Caciuloui, for that deliberation and what you have actually told the Committee. The Committee takes note of all those things that you have said. I will now open the floor for the Honourable Members if they have need to sought any clarifications or ask questions.

HON. R.R. SHARMA.- Mr. Chairman, I would like to thank the presenters. It was a detailed presentation and I do not have any further comments on that, thank you.

MR. CHAIRMAN.- Thank you, Honourable Sharma. Honourable Dr. Salik Govind, do you have any comments?

HON. DR. S.R. GOVIND.- Mr. Chairman, I would like to thank the presenters for a very comprehensive but very informative view on the subject matter. It had really opened our eyes more and broadened our thoughts. I think we need is a little bit of time to deliberate on all the submissions, as a lot of questions will come to our mind which we can put to the presenters again in writing. To me personally, it is a very, very useful presentation. At this stage, I would like to especially thank you all for the very comprehensive insights into the subject matter.

MR. CHAIRMAN.- Mr. Hunecke, do you have any comments or any input you would like to share?

MR. T. HECKNE.- Mr. Chairman and Honourable Members, I have nothing further to add but just reiterating the words of my two colleagues. We are extremely grateful and feel privileged that we are able to interact with you and the time given to us, so many thanks to you, Mr. Chairman and Honourable Members of the Committee. Thank you very much.

MS. N. KARAN.- Mr. Chairman and Honourable Members of the Committee, we would like to especially just wish to thank you again for the extension of time that was given to provide these submissions and allowing us to make these submissions to you and presenting these online. We stand ready to assist your office if you need some clarifications after reading our submissions in more detail and after deliberating amongst yourselves.

We will provide those explanatory notes to the Budapest Convention for your noting, so perhaps we will email your officers that document to be disseminated to your good selves. If you require any more guidance, we are able to provide the documents as stated in our submissions as well. So many thanks for your time and many thanks for the attention given.

MR. A. CACIULOIU.- Also, I would like to thank you for the opportunity in participating and if there are any other questions, I would be more than happy to provide them in writing.

MR. CHAIRMAN.- Thank you Presenters and thank you Honourable Members for the presentation today. I was very detailed and thorough in nature and the Committee has definitely taken note of the submission and the points that have been raised, so now we will get into Committee stage and discuss these and if there is any further clarification that we need to seek from the Presenters, we will be writing again to you or we might actually have another virtual meeting to get clarifications. We will also write to the drafters as well, seeking their explanation on the points that have been raised during the submission and we will see what their explanations are and what do they think about the submission that was given today.

Once again, thank you very much to you all.

The Committee adjourned at 11.37 a.m.