[VERBATIM REPORT]

STANDING COMMITTEE ON JUSTICE, LAW & HUMAN RIGHTS

BILL

Cybercrime Bill 2020 (Bill No. 11 of 2020)

INSTITUTIONS: (1) University of Fiji
(2) Ms. S. Tamanikaiwaimaro
(3) Fiji Women's Rights Movement (FWRM)

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

DATE: Thursday, 25th 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 THURSDAY, 25TH JUNE, 2020 AT 9.20 A.M.

Online Interviewee/Submittee: University of Fiji

In Attendance:

(1)	Professor Shaista Shameem	-	Vice-Chancellor
(2)	Ms. Varsha Feriyal Bano	-	Lecturer in Law
(3)	Mr. Shivendra Nath	-	Lecturer in Law
(4)	Mr. Joseph I. A. Camillo	-	Head of Campus, Samabula
(5)	Ms. Kesaia Tuikoro	-	Law Librarian

MR. CHAIRMAN.- Honourable Members, members of the media and the general public, the Secretariat team, dear viewers, ladies and gentlemen; a very good morning to you all and it is a pleasure to welcome everyone, especially the viewers who are watching this session.

For your information, today's submission will be made available to the public through the media and also on television through the Parliament Channel on our Walesi Platform. I am kindly advising that any sensitive information concerning this inquiry that cannot be disclosed in public, if this can be provided to the Committee either in writing or in private.

At the outset, I request our witness and wish to remind Honourable Members that all questions are to be asked and addressed 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 meeting, kindly request that there be minimal use of mobile phones and that all mobile phones are to be on silent mode while the meeting is in progress.

(Introduction of Honourable Members by Mr. Chairman)

Joining us today are the representatives from the University of Fiji; the Acting Vice-Chancellor - Dr. Shaista Shameem, Mr. Joseph, Mrs. Varsha Bano, Mr. Shivet and Ms. Kesaia Tuikoro. I shall now invite our representatives from the University of Fiji to introduce themselves before we start the submission.

PROFESSOR DR. S. SHAMEEM.- Thank you very much, Honourable Chairman and Honourable Members of the Standing Committee. My name is Professor Shaista Shameem and I am the Acting Vice-Chancellor of the University of Fiji, as well as the Dean of the Justice Devendra Pathik (JDP) School of Law at the University of Fiji.

MR. S. NATH.- My name is Shivendra Nath. I am also a lecturer at the University of Fiji and I specialise in the area of criminal law, evidence and taxation. Thank you.

MS. V.F. BANO.- Good morning, Honourable Chairman and Honourable Members of the Committee, ladies and gentlemen; my name is Varsha Bano. I am a lecturer in law at the University of

Fiji JDP School Of Law. I teach courses that include but are not limited to criminal law, process and procedure and advocacy-related courses. Prior to becoming a lecturer in law, I have been a legal practitioner, practicing criminal defence. Thank you.

MR. CHAIRMAN.- Thank you. Now I give the floor to Professor Shaista Shameem, if she can take us through the submission that they have before them. Thank you.

PROFESSOR S. SHAMEEM.- Thank you very much, Sir. Mr. Chairman and Honourable Members of the Standing Committee, we have divided our submissions into three parts. I hope you have written submissions as well. We have sent them to the Secretariat yesterday, so if there are any questions afterwards, please feel free to address us on those.

I am going to generally speak about our overview and speak about the Constitutional provisions that, I think, are very important when considering a Bill of this nature, the Cybercrime Bill 2020.

One of the aspects of the proposed legislation that concerns me a little was Clause 17(2) of the Bill, which is very broad in terms of the protection that it can provide for people who have been either charged or are about to be charged in relation to the privacy of other information or other confidential information, then that can be exposed if the warrant is applied for with respect to a court or judge. So, that is my first concern.

I refer to the Constitutional provisions, Section 24 in particular - Right to Privacy, but more importantly, there is a provision in the Constitution on interpretation in Section 7(1)(b) which states, and I quote:

> "In addition to complying with Section 3 and applying this Chapter, a court tribunal or other authority may it provide relevant consider international law applicable to the protection of the rights and freedoms in this chapter."

And the only freedom and right that is provided in the Chapter which is the Bill of Rights Chapter, is the right to privacy.

Now, the right to privacy also has limitations. So, if there is a law that is passed limiting the right to privacy, that law has to be taken into account in a court or tribunal or before any other authority. Unfortunately, the Section that I referred to is too broad in terms of providing that protection which an individual is entitled to have when this particular provision is employed in regards to someone who is reasonably suspected of committing a crime that would be contained within the Cybercrime Bill 2020.

The specific document that we have already attached as well to our submission is what we call the Siracusa Principles. The Siracusa Principles come as an attachment to our submission and I respectfully invite the Honourable Members to look at those principles and the full title is Siracusa Principles on the Limitations and Derogatory Provisions in the International Covenant on Civil and Political Rights. This is specifically possible in political rights and the Cybercrime Bill 2020 immediately brings to bear civil and political rights that are also protected in the 2013 Constitution of Fiji.

With respect to the limitation, essentially what the Siracusa Principles tell us and it is a United Nation's document is that, every country has the right to limit the Bill of Rights provisions, whatever they may be. So, freedom of movement, freedom of expression, freedom of association, et cetera, are not blanket rights, they can be limited in the case of a national emergency. For example, in public health situation, the number of national security, all of those things can actually limit a particular freedom or a particular right.

However, Siracusa Principles tell us that there is actually a limitation on the limitation as well. So if you are going to be limiting anyone's rights, you are also, at the same time, have to ensure that the fundamental rights itself is not undermined as a result of that limitation. So, for me, as a constitutional lawyer and as a human rights lawyer, my concern is Clause 17(2) of the Bill because it is very wide in respect of the power that it provides people in authority and specifically, Clause 17(2) says, and I quote:

> "The powers and procedures provided under this Part are without prejudice to the operation of, or powers granted under any written law, when exercised lawfully by a police officer or other authorised person, or at any regulatory authority that by itself does not investigate or prosecute an offence."

The words, "….are without prejudice to the operation of…", is of concern because it is ambiguous. It is not clear whether this means it involves the Constitution as well. "… without prejudice to the operation of, or powers granted under any written law…", and the Constitution is any written law. So that is the Clause that, for me, has actually triggered the Bill of Rights concerns that are also provided in the Constitution.

As I have said, the Constitution itself does give limitations to certain rights, so practically in all of the rights, there are limitations. But one needs to interpret 'limitations' in accordance with the Siracusa Principles. So those are the issues that I have for you, Honourable Members. Perhaps, if you would like to ask questions now or perhaps, we will do the entire presentation, because my colleagues will be looking more specifically at the other provisions of the Bill. Thank you.

MR. CHAIRMAN.- Thank you, Professor, for that deliberation. If you were actually to change the wordings of Clause 17(2), how do you actually do it? What changes do you recommend to that particular Clause, if there is any?

PROFESSOR S. SHAMEEN.- I would make it more specific, so rather than saying, "…without prejudice to…", I would say, "…in compliance with …", and refer to the specific provision in the Constitution, or broadly the Constitution itself rather than a specific provision like Section 24, because Section 24 does provide limitations.

The problem is, of course, to what extent can a limitation operate? And the Siracusa Principle says that you can have limitations that would undermine the right itself and that, in fact, in international law is not permitted. So I would be very specific and I would say, "…in compliance with 2013 Constitution of Fiji…", and perhaps, also remove the words, "without prejudice".

MR. CHAIRMAN.- Thank you for that. We will move forward. Honourable Members, any questions or queries for Professor?

HON. R.R. SHARMA.- All good so far, you can keep on going.

MR. CHAIRMAN.- All right, we will continue. Our representatives from the University of Fiji, you can continue.

MR. S. NATH.- Very well, Mr. Chairman. I will be focusing on the second aspect of the submission that we had drafted. If you look at the introduction, it talks briefly about, what is cybercrime and what is digital evidence.

The basic premise of the introduction is that, cyber evidence or digital evidence is much more different from the real evidence that we deal with in the Court of Law. It is different from the real evidence - exhibits that you find in the police station.

The major premise of presenting this evidence to court, depends on the authenticity of the evidence. So there are three points that I have highlighted in the introduction, which talks about what type of evidence is digital evidence. It talks about degradation, ownership and the original documents.

This leads on to Part 5 of the Bill, which says, "… on search warrants…". In order to authenticate these sets of evidence, the drafters must clearly state as to what mechanisms are to be used in extracting this evidence from a computer system or from a computer data.

Therefore, if you look at Clause 2 and Clause 16, we are humbly pleading that another clause to be added which talks about something which is in the interest of justice and in compliance with the European Convention on Human Rights which says; "there are private rights, however, there are exceptions and these exceptions only work or should be made when it is in regards to public safety, security issues to protect fundamental freedoms of the public, et cetera."

Therefore, the proposition is, under Clause 16, there must be another subsection which looks at how the judge or magistrate looks at in issuing warrants and being specific as to the steps taken in terms of acquiring this data because of the digital evidence at play here. That is the first point that I would like to make, so that it is in compliance with Section 24(2) of the 2013 Constitution and it is in compliance with the European Convention on Human Rights which says, if it is to be limited, it must be with regards to public rights, public safety, et cetera. I am specifically referring to the European Convention on Human Rights which Fiji is a signatory to and it is also stated in our Constitution, so that we are in compliance with the international law and with the Constitution as well, as our Professor had stated.

The second point, Honourable Chairman, is on mobile phones and cell phones. Now, the Bill is not very clear on the definition of computer devices or what is a device. Therefore, it can be deliberated and it is a proposal that mobile phones and cell phones are also to be included in the devices section.

I have stated there what is the proposal because mobile phones and cell phones are also used to coordinate crimes or cybercrime. This can relate to cyberstalking, cyberbullying, and crimes of cyberterrorism, identity theft and embezzlement. The proposition as to why mobile phones are used is because it can be coordinated just like a computer, however, we have to tread in this area very carefully because of privacy issues. Therefore, again, it should be in compliance with the Constitution, and the judge and magistrate must be able to ascertain what the reasonable cause is when issuing a warrant.

Basically the two propositions are on the issuance of warrant and the steps taken whilst extracting information from the mobile phones or cell phones and in checking documents of a particular perpetrator in regards to public safety and security issues. That is all, Honourable Chairman. Thank you.

MR. CHAIRMAN.- Thank you, Sir. Thank you for the deliberation. Any clarifications, Honourable Members?

If none, then we will move forward to the third part of the submission now.

MS. V. BANO.- Honourable Chairman and Honourable Members of the Standing Committee, ladies and gentlemen; my submission is based on Part 3 of the Cybercrime Bill 2020 which deals with computer-related and content-related offences.

With respect to that, we have noticed that there are two things that the current Bill is lacking. These include emphasis on the crime of hate speech online and cyberterrorism. And in my submission, I will attempt to explain why Parliament should consider this to be a part of the Cybercrime Bill 2020. Why it is important to be implemented under this legislation.

The dangers of cybercrime have always existed. It has existed for many years and it is not uncommon for cybercriminals to attack the network system of individuals. With the COVID-19 outbreak, this is no exception to the situation.

Cybercriminals constantly look for different ways to take advantage of online behaviour and trends which relate to cyber-attacks. At this point in time, with the increase in the percentage of the population connected to the internet and the time spent online, countries all across the globe are reporting an increase in cybercrime.

Currently, Fiji has laws that deals with content that is aimed at causing harm to a person's reputation, content that can cause harm to the computer system of an organisation or a person. But these are very limited in nature, we can find them in the Crimes Act and we can find them in the Online Safety Act. They do not have a jurisdiction that has principles that calls for international co-operation. So we are of the view that any Cybercrime Bill that needs to be passed by Parliament should include the areas of hate speech online and cyberterrorism.

Hate speech has been defined in our current Constitution and Section 17 is important to this because this section talks about freedom of speech. Freedom of speech, freedom of expression, freedom of publication and freedom of opinion are all expressed in the Constitution, but they do not advocate coherent or they do not offer protection in where such freedom constitutes incitement to cause harm.

Our submission is that with hate speech if it has expressed through an online platform, it has the potential to do more damage because the way in which the information is disseminated, unlike contravention channels, the dissemination of hate speech online often involves multiple actors and multiple platforms, and the content is likely to stay available until discovered by law authorities. So given the protection that freedom of speech under Section 17 offers, a person should not be able to come and use the online platform to promote hate speech. They should not be able to promote offences of xenophobic nature and rely on this Section as a blanket to cover that.

What we are saying is that the law should take Section 17 of the Constitution into consideration and include those principles in the current Cybercrime Bill so that those principles that recognise hate speech, that attacks on the dignity of individuals, groups of individuals or respected officers, this kind of protection is offered under the Cybercrime Bill 2020 and a person should not be allowed to use freedom of expression to carryout offences of this kind of nature because the online platform is really big. They could do anything on the online platform. They could put up any sort of material and rely on this particular Section as a cover up, so that is what we are submitting, that Section 17 of the Constitution which prohibits hate speech should be considered and should Parliament find appropriate, the offence of hate speech be created under the content-related and computer-related offences of the Cybercrime Bill.

My second point is in relation to cyberterrorism. This is another offence that we submit, Parliament may look at and consider including in the current Cybercrime Bill 2020. Cyberterrorism is a complex area, however, if you really analyse cyberterrorism and you get down to understand how it operates, you will realise that cyber-terror against a country and its citizens can take place at a number of levels of sophistication. The simplest level of cyberterrorism attacks are the kind that deny service and disrupt the daily life, with no such substantial irreversible or lasting damage, whilst the highest level on the scale could be an the attack on organisations' core operational and operating systems.

The cybercriminals may attack certain crucial computer networks, which possibly caused a disruption of essential public services, such as water, power, hospital systems, financial systems and emergency services.

The modern cyberterrorist may be able to do more damage to the use of a keyboard, then that would …..(inaudible)…. So, this kind of attacks cause a havoc on the infrastructural information and computer networks. It also brings devastation to the nation's economy, security and public welfare in the physical work. Countries such as United States of America, India and Pakistan have all experienced this and they are now tirelessly working towards implementing laws that protect them from an offence of cyberterrorism. And I have in my submission a draft of what the law would look like - the elements of the offence, if it were to be implemented under this particular Cybercrime Bill 2020.

So, with respect to the point on cyberterrorism, we cannot underestimate the threat that it poses to our infrastructure. We understand that Fiji has been working towards ensuring a safer cybercrime for all. The draft Cybercrime Bill 2020 is here and it will take us a step further towards achieving this objective.

We are humbly submitting to Parliament on this point to consider incorporating laws that deal with cyberterrorism. As the presence of the stringent laws that deal with this kind of offences, it will not only act as a deterrent but it will also enable us to protect our country and its people when the need arises.

Given the COVID-19 situation and the trend whereby people are moving online now as everything is done online, we have to prepare ourselves and we have to, whether we feel that we are facing the threat significantly or not, regardless of that. We need to have that in the legislation so that in the future if we are faced with this threat we are prepared. That is the end of my submission, Mr. Chairman. Thank you for listening.

MR. CHAIRMAN.- Thank you, Ms. Bano, for that comprehensive deliberation with regards to the Cybercrime Bill 2020. I believe all the sections that you have mentioned, we have taken note of

them, and we shall be discussing them once we sit in the Committee stage for the deliberation of all the submissions. Any final words from the submittees?

MR. S. NATH.- Just one point, Honourable Chairman, in terms of the European Convention on Human Rights, our proposition is actually aligned to whatever is in the European Convention on Human Rights and the internationally disputing too when deciding cases in the court of law. Therefore, the proposition is in regards to that and specifically regards to Section 24(2) which states, and I quote:

> "If we are to limit or exercise our judicial state discretion against private rights it must be done very carefully and in accordance with the Constitution and international law."

That is our submission and that is the basis of the search warrant and ….(inaudible)…. Cyberbullying because of the issues of privacy. Therefore, a balancing act has to be done between public rights and private rights, and that is the crux of our submission. That is all, Mr. Chairman and Honourable Members. Thank you.

MR. CHAIRMAN.- Thank you, Sir. I will open the floor now and if the Honourable Members have any questions or clarification they would want to seek from the representatives of the University of Fiji.

HON. DR S.R. GOVIND.- Thank you, Honourable Chairman. I would like to thank the presenters for a very comprehensive presentation with lots of new of things that we did not know. I think we will deliberate on those and try to incorporate into our submission at Committee level. At this stage, I do not have any other question but if we do then, we will write over to Professor Shameem and seek clarification. Once again, thank you for your input in today's very important Bill.

PROFESSOR S. SHAMEEM.- Thank you very much, Sir. Just as a final word, if I can just ask the Honourable Members to look at the Siracusa Principles because it is very easy. This is the United Nations document already. It is very easy to take care of all the issues that we have spoken about with respect to constitutional protection, and include that as a reference as well.

So, if you would like to be further informed of the limitations clauses because it is relevant, not only for this type of legislation which is to combat a particular crime which everyone agrees ought to be combated for the reasons that we have said, but also in relation to any other proposed Bill that may come before the Standing Committee on Justice, Law and Human Rights.

With respect to paying heed to the constitutional provisions which protect rights but at the same time, provide limitations which allow Government or the State to put in place certain legislation to limit those rights. But as I have said before to reiterate, the limitations themselves have limitations in international law. So, thank you for the opportunity to talk about them.

MR. CHAIRMAN.- Thank you, Professor. Honourable Sharma, any final comments?

HON. R.R. SHARMA.- Thank you, Honourable Chairman. I would like to thank the presenters this morning for their detailed submission. Definitely, we will come back on this when we meet during Committee stage, and if we have further queries on this or we would want to know some other details, we will definitely come back to you on that.

(Vote of Thanks by Mr. Chairman)

Once again, thank you very much and hope to see you in a near future.

PROFESSOR S. SHAMEEM.-Thank you.

The Committee adjourned at 9.52 a.m.

The Committee resumed at 10.29 a.m.

Online Interviewee/Submittee: **Ms. Salanieta Tamanikaiwaimaro**

MR. CHAIRMAN.- Thank you, Honourable Members, members of the general public, the media, secretariat team, dear viewers, ladies and gentlemen; it is a pleasure to join you on this live telecast of our second submission today on the Cybercrime Bill 2020. It is a pleasure to welcome each and every one of you who are joining us live today. Thank you very much for that.

As mentioned in today's earlier submission, this submission will also be made available to the public through the media and television through our Parliament Channel on our Walesi Platform. Therefore, I am kindly advising that any sensitive information that cannot be disclosed to the public, it can be given to this Committee either in private or in writing.

This Parliamentary inquiry and all information gathered is covered under the Parliamentary Powers and Privileges Act. In terms of the protocol of this Committee meeting, kindly requesting that there be minimal use of mobile phones and all mobile phones are to be on silent mode while this meeting is in progress.

(Introduction of Committee Members by Mr. Chairman)

Today, the Committee will be hearing submission on the Cybercrime Bill 2020 and joining the Committee today is Ms. Salanieta Tamanikaiwaimaro. I now invite Ms. Tamanikaiwaimaro to present her submission. Please, note that if there are any questions by Honourable Members, we may intervene or interject in between or if not, then we will leave all the questions and answers t the end of the submission.

Thank you Ma'am, you have the floor now.

MS. S. TAMANIKAIWAIMARO.- Thank you very much, Honourable Chairman. I thank you for the opportunity to be able to comment on the Cybercrime Bill 2020.

Firstly, I would like to congratulate the Committee in inviting the general public to comment on the Bill in its current form and I have the privilege to be able comment and also to address the Committee.

In terms of the written submission I had sent, I would just like to comment on a few pertinent things that I feel the Committee could look at. Firstly, I am glad to see the Cybercrime Bill 2020 and it is critical because the current legislation is clearly not able to penalise various offences. This is the gap.

I would just like to see that traditionally when cybercrime takes place online and the two overarching areas of cybercrime; one being cyber dependent which can only be committed through the use of online devices or whether the devices are the tool; and the other one is cyber-enabled - the traditional crimes that can be increased in scale by using computers.

I have also submitted a paper that I wrote in 2010 called, 'Cybersecurity in the Republic of Fiji', whereby on pages 13 and 14, I made a comparative analysis from various jurisdictions' cybercrime offences. In pages 13 and 14, you will see Australia, the United States, et cetera.

When you see the way the Bill is currently worded it, sort of, mirrors the European categorisation. As you can imagine, when I gave that categorisation that was way back in 2010. So, 10 years onwards, you will still see the gaps that were highlighted in the table.

What I have done is, I have updated it to factor in the Online Safety Act and also the United Kingdom's categorisation. You will see that the Online Safety Act 2018 is primarily based on a sub-set of content-related offences, which typically falls within cybercrime, and you will see that in the submission I sent you. If you could refer to the annexure, it will show the different categorisation, but we will come to that later on. But suffice to say that the table is there for your technical purview and it will show you the offences that have yet to be inserted into the draft and those are the ones that are left blank in the last column in the table.

For now, I would like to comment on the interpretation provision in terms of 'authorised person'. I would say that it should include the Office of the Director of Public Prosecution and the Online Safety Commission and in future where bodies are created specifically to deal with this, I would widen this from Police Officer to Law Enforcement Officer. The reason why I say this is because the Cybercrime Unit sits within the Fiji Police Force and traditionally, it is the DPP that prosecutes cybercrime offences in Fiji. At the moment, it is computer-related offences.

In terms of the interpretation of 'Minister', because the Police is part of the disciplined services of Fiji, I would submit that the interpretation should read that Minister should Minister for Defence, as policing is a law enforcement issue. The Ministry of Communications, I respectfully submit is responsible for setting policies and regulating telecommunications and licensing internet service providers and telecoms.

Having said that, obviously in terms of the telecommunications regulations, those that are enforced by the Telecommunications Authority of Fiji (TAF). But in terms of the cybercrime offences, it is traditionally been the remit of the Fiji Police Force.

What I have done is obviously there is cooperation and collaboration amongst diverse agencies as is with all these. So, to show this relationship, I refer to paragraph 11 of my written submission where you will see I did a jurisdictional map. You can see the coloured circles for graph 11. Can you see it?

MR. CHAIRMAN.- Yes.

MS. S. TAMANIKAIWAIMARO.- The image was done way back in 2010 so obviously, I could not update it but traditionally, those agencies still are the same agencies. So, I would submit that FICAC's remit is corruption offences whereas in terms of prosecution of all corruption offences and the DPP has a wider scope. But in terms of law enforcement, I would submit that as is currently it is within the Fiji Police Force. Obviously, you will see the overlapping jurisdiction between the Police, working in collaboration with the different Ministries, the different agencies, so I have showed both, the domestic, national and regional.

The other interpretation that I had referred to is the term, 'serious offence'. So damages caused by certain cybercrime can amount to millions of dollars in damages. When we did five years' worth of national consultation, some of the damages were massive and it went way beyond $500. For instance, when certain people who were abroad, sort of, invaded because of confidentiality, like a private institution, but the cost was hundreds and thousands of dollars. Obviously, the institution's overseas insurance covered the loss but to penalise and say $500 and 6 months for serious offences. So, there has to be a reasonable tariff in terms of a reasonable spectrum, minimum and maximum.

The other thing that I would like to submit is that, there needs to be a distinction between summary offences, either way offences or indictable offences.

In terms of the definition of 'service provider,' the way the Bill is currently drafted is just limited to offences that are restricted within computers. But I would submit that because you have things, like telecommunication services, that it should be broadened. And "service provider" should be expanded to say, "…an entity that provides access to the Physical Layer, Transportation Layer and Application Layer of the internet. In other words, what I am talking about is the cyber environment and there has to be a definition of what a cyber environment is.

All those people who are prosecuting will have to specific because there are certain offences that can happen where we do not need a computer or a device to pull up the crime. I remember having to go to Christchurch to investigate a numbering theft. Sir, you know, it is quite diverse, whether it is spectrum or interference along the fibre cables. Take for instance, a private company is doing surveillance along the fibre cable. I would submit that there has to be a definition of cyber environment and a wider definition for "service provider".

Sir, for the Committee's ease, I have defined it in paragraph 13 of my submission and I have also put an illustration, which is actually from page 35 of Jovan Kurbalija's book, *An Introduction to Internet Governance*. So it has the infrastructure which is the Physical Layer at the bottom, which includes the submarine fibre cables, telecommunications towers. It includes the Transport Layer, which is the Protocols, where the computer networks is and it includes Content and Application. In Content and Application, we have referred to that earlier where the Online Safety Act covers some of it, but the others that are not covered by it, should be covered within the Cybercrime Bill 2020.

The Content and Applications Layer can include things, like ATM machines, computers, so if we are just creating a law or defining the cyber environment as limited to one layer, we will become limited and so it will be hard to prove the other offences.

MR. CHAIRMAN.- Madam, in one of the submissions we received from one of our submittees, they were actually proposing that the "service provider" definition should be narrowed to the service provider only. You are saying here that it should be broadened to cover everyone and I think that was the interpretation at that point in time, that the current definition of "service provider" actually covers all those things, such as ATM machines, et cetera.

MS. S. TAMANIKAIWAIMARO.- I would respectfully submit that if it is not defined within the Bill, people can get away with it easily. The three layers that I am showing here - Physical Layer, Transportation Layer and Application Layer, those are the cyber environment. So when we say "service

provider", we could say, which service provider? Are we talking about the internet service provider? So, it is just that level of specificity.

MR. CHAIRMAN.- All right.

MS. S. TAMANIKAIWAIMARO.- Feel free that at any point further to the deliberation, if there is any request for clarification, I will be happy to come on again.

It is important to note that in order to adequately prosecute theft of telecommunication services, espionage in submarine cables, let me give an example. There are countries in the Pacific or territories where the US Government completely forbids certain vendors from coming into the site to install routers and those routers are not even computers. The reason for it is that it has capacity to resend and recapture information, like criminal-related information for surveillance purposes.

So for that reason whether it is the UK, whether it is NATO there in Europe, whether it is American in American territories, you will see that they forbid certain companies. Usually it could be the Chinese companies, not that I have anything against China, I love the Chinese people, I went to a Chinese school but what I am saying here is, there is a need to broaden the definition of a cyber environment from just computer because if you are not specific, it is very easy to defend the charge. Does it make sense?

MR. CHAIRMAN.- Yes, it does.

MS. S. TAMANIKAIWAIMARO.- Let us move on. A lot of my submissions are written already, it is easy for you, but I am just picking up what I feel is critical. Are there any questions for me at this point before I move on to the next bit?

MR. CHAIRMAN.- Do you have any questions, Honourable Members?

HON. R.R. SHARMA.- So far all good.

MR. CHAIRMAN.- Yes, Honourable Dr. Govind.

HON. DR. S.R. GOVIND.- It is alright with me. Thank you, Mr. Chairman.

MR. CHAIRMAN.- We can continue, Madam.

MS. S. TAMANIKAIWAIMARO.- Let us continue. So, the other thing I noticed with the Bill, the way it is currently drafted, it is limited to Fiji citizens and Fijian jurisdiction. I would go further to submit that majority of the offending is actually taking place where the victims are actually Fiji citizens, it is taking place within the cyber environment but they are not necessarily Fiji citizens, like the perpetrators …

MR. CHAIRMAN.- Yes.

MS. S. TAMANIKAIWAIMARO.- … whether it is the ones who are creating a malware …

MR. CHAIRMAN.- You mean to say someone is sitting somewhere else and committing these crimes in Fiji.

MS. S. TAMANIKAIWAIMARO.- Absolutely! And for that reason, I would submit that Clause 3 in terms of application should be broadened to capture them. I have mentioned it in Paragraph 15 of my submission, and I have also referred you to a country which the world considers as one of the leading super-connected world, who were very stringent on cyber-attacks and cyber defense. In fact, the Americans are mentored by the Estonians I would say or at least when His Excellency, the former President of the United States of America, Mr. Barack Obama, was in office, Estonia would be official advisor for the United States.

So you will notice that the link that I have mentioned, this presentation made by the Estonian Government where they had, in the link that I have sent which is hyperlinked into this submission, they definitely had experienced weaknesses in cases in terms of prosecution because they felt that the law was not specific enough, or it was not adequate, or the penalty was not serious enough. It certainly did not match the offences.

In Paragraph 16 of my submission, I go to what I had referred to initially in terms of the categorisation. I apologise it might be a bit dry, but it is the annexure. Let me know if you can see it.

MR. CHAIRMAN.- This is the first one. Are you talking about the table?

MS. S. TAMANIKAIWAIMARO.- Yes.

MR. CHAIRMAN.- Alright, yes.

MS. S. TAMANIKAIWAIMARO.- The annexure table showing categories of cybercrime by jurisdictions. What I have done is, I have compared it to Fiji's categorisation in terms of existing domestic law, and then I have also analysed it with the Cybercrime Bill. So the places where you see domestic laws where it is blank and then you will see it, the Cybercrime Bill 2020 where it is blank. Can you see?

MR. CHAIRMAN.- Yes.

MS. S. TAMANIKAIWAIMARO.- Those are things that are, sort of, missing from the Bill.

MR. CHAIRMAN.- So, you mean to say, for example, number two – computer-related traditional crime?

MS. S. TAMANIKAIWAIMARO.- Yes, for example, number two – computer-related traditional crime, you can see it in section 340 and section 346 of the Crimes Decree..

MR. CHAIRMAN.- Alright.

MS. S. TAMANIKAIWAIMARO.- For example, fraud. Fraud happens and it is a traditional crime. But if it happens online, that would be perceived as computer-related traditional crime.

In terms of content-related offences, I mentioned that with content it is a very big umbrella. A subset of that content is actually mentioned in sections 24 and 25 of the Online Safety Act, particularly in relation to what the Indian legislation in India refer to as 'riding' or we refer to it as bullying or harassment online or trawling. But there are other aspects of content that could be covered.

In cybercrime, infringement of privacy, we do not really have appropriate offences in relation to that. Let me give an example. The computer that you have in front of you, the fact that we are using this platform to talk to each other, you can see me and I can see you, right?

MR. CHAIRMAN.- Yes.

MS. S. TAMANIKAIWAIMARO.- When our computer is switched off because we are globally connected once we are on the network, anyone can hijack your camera and spy on you, and watching. Even when your computer is switched off. So you can be part-naked or moving around or doing whatever in your home and someone can violate your privacy by coming into your bedroom through your machine. So does this make sense?

MR. CHAIRMAN.- Yes, it does.

MS. S. TAMANIKAIWAIMARO.- That is not yet in the Cybercrime Bill 2020. So that is why it has a blank there. I am going according to categorisation and comparing different jurisdictions.

Then obviously, you have got the Australian category. The Australians have got different categories. Before I go to the Australian category, I just want to say that in different countries, you will see they have these different categories. The reason for that is, just like my dress, it will not fit Sushila in Fiji because they also have other laws that run in tandem that may address certain things. So just to rely on the European categorisation, we would err if we did not do the comparison. So this is already done so it will make your work easy and just for you to consider.

So going to the Australian, for instance, you got Telstra Telecommunication Services, so this has never been covered in Fiji. It is good to see that it is going to be covered under section 12 of the Bill.

And you have got things like, "communications in furtherance of criminal conspiracy", we do not have that. "Telecommunications piracy", why would we not have some aspects of it in the Copyright Decree? We do not really have that, and it does not have to be called, "telecommunications piracy", it could be just "piracy" alone. Dissemination of offensive material, obviously that is covered in the Online Safety Act. Money laundering is already covered.

The other thing that is not covered is "electronic vandalism, terrorism and exhortation." Terrorism is covered in the Crimes Act. If I were to give you an example of electronic vandalism, for example, Mr. Jones from Tonga hijacked the Parliament website and you had private content which the Speaker or the MPs would be accessing your own private data group, and you are unable to access it because all you would see are swear words and graffiti, or like your leader in diapers, or an MP with a bottle of milk, like to make fun. You notice, like how you do vandalise a building?

MR.CHAIRMAN.- Yes.

MS. S. TAMANIKAIWAIMARO.- Believe it or not, it has actually happened to the Government websites in the past but not to that extent where they put illustrations but they certainly defaced the website. But it is not something that people really like to really talk about because people like to pride themselves on security. You can see when we go through the table, there is quite a long list. You have got the US categorisation, trafficking in passwords is not an offence in our Bill. Can you see?

MR. CHAIRMAN.- Yes.

MS. S. TAMANIKAIWAIMARO.- And it is for the Standing Committee from Parliament to say, "Alright, which ones do we want". But as is currently, I would say that you need to include to be robust because there is no point in coming back and forth in amending later when you can get it right now.

So, one of the things that I have added for your ease of reference there were two documents that I had sent, as I mentioned:

(1) my submission; and
(2) the paper I wrote in 2010 which provides an overview for anyone who may not necessarily understand the connections, it will just make it easy reading - very, very light and easy reading.

Another thing that is not covered is distributed denial of service attack, dark web where the hackers go. The other ones are covered, like identity theft is covered under Clause 11 of the Bill. From Clauses 5 to 11, it is covered under Online Safety Act, and that is what I was referring to the subspecies.

Now, in terms of UK's 13 categorisation, I would submit that we do not need to codify that because we have villages that do not have proper libraries - in the outer islands and rural areas, and they rely on the internet, they rely on the second-hand information, et cetera, virtual information, online content.

You would obviously be receiving so many submissions and there will be people talking to you about sentencing, tariffs and the legal aspects. That is why I did not want to go too much into it because I know they are going to do it. But what I would like to say is, for first offenders, particularly kids, we have up and coming kids who are bright, and innovated, like 14 years old or 12 years old and they learning to manipulate protocol and phones. So, if they were to be caught in certain things, just a redemptive and rehabilitative aspect to channel that innovation so that they are not grossly penalised because they have a whole future ahead of them. You know, like channeling that capacity to innovate. I understand that Fiji has a digital strategy and so part of it is growing a broader human capacity.

Essentially, those are the gist of my submission and I am happy to take any questions or comments.

MR. CHAIRMAN.- Thank you, Madam, for that in-depth deliberation with regards to the Cybercrime Bill 2020 itself. The table that you have provided gives a very good insight and definitely, we will be going back to our drafters to get their views as to how this ones can be incorporated or if there was any reasons for this kind of things to be left out from this particular Bill, or if it covered somewhere else as that might be one of the reasons as to why it is not covered in this Bill. But it provides a very

good overview for the Committee to actually look into these things that are not covered. The points that you have mentioned are well taken on board.

I will open the floor now for other Honourable Members, if they have anything they want to bring up or get clarification on with regards to the Bill?

HON. DR. S.R. GOVIND.- I would like to thank the presenter for a very comprehensive presentation. A lot of new areas have been highlighted and definitely, we will deliberate at Committee level and if it is not incorporated and the reasons to incorporate or we will corporate in the Bill. So, that is all I have, and I would like to thank the presenter again.

MR. CHAIRMAN.- Thank you, Honourable Dr. Govind.

HON. R.R. SHARMA.- Thank you, Mr. Chairman. I would like to thank, Madam, for your timely submission. Definitely, we will come back to you as we meet inhouse and we will just collaborate all the submissions you have provided from your side, we will have some queries or some questions when we will see the soft copy and hard copy of it, which is in front of us, then definitely we will come back to you if we have any information we need from you. Otherwise, thank you very much.

MS. S. TAMANIKAIWAIMARO.- Thank you, Sir.

MR. CHAIRMAN.- Thank you. Once again on behalf of the Committee, Madam, thank you very much for availing yourself to today's presentation. As alluded to earlier, a very insightful submission from you and thanks a lot for taking out your time. Now, we shall have final comments from you before we close this submission.

MS. S. TAMANIKAIWAIMARO.- Thank you, Sir. My final comment is the issue of jurisdiction which I canvas in the submission in terms of who is going to be enforcing it. That is something I leave to you and the relevant Ministry and the drafters and the drafting instructions, because when drafters draft, they have to receive drafting instructions from the relevant line Ministry. For instance, cybercrime if I remember correctly, there was a Cabinet directive back in 2011, way back when they had wanted a cybercrime legislation. So, that is just something for you to consider. But other than that I would like to thank you Sir and Honourable Members of the Committee for allowing me the opportunity to address you today.

MR. CHAIRMAN.- Thank you, Madam and viewers. We shall take a 10 minutes break now before we actually go into our third submission. *Vinaka vakalevu*.

The Committee adjourned at 11.02 a.m.

The Committee resumed at 11.29 a.m.

Online Interviewee/Submittee: **Fiji Women's Rights Movement**

(1) Ms. Artika Singh - Team Leader and Transitional
(2) Ms. Bernice Lata - Legal Rights Officer
(3) Ms. Laisa Bulatale - Research Officer

MR. CHAIRMAN.- Thank you, Honourable Members. Good morning ladies from the Fiji Women's Rights Movement (FWRM). Firstly, I would like to welcome each and every one of you back to our third submission for the day. It is a pleasure to welcome everyone to this session.

As mentioned in today's earlier submission, this submission will also be made available to the general public through our Walesi Platform. Therefore, I am advising that if there is any information that cannot be disclosed in public, that can be given to us in writing or in private. Also, all inquiries are conducted under the Parliamentary Powers and Privileges Act.

In terms of protocol, we will request that all mobile phones be switched to silent mode while we are having this particular submission.

(Introduction of Committee Members by Mr. Chairman)

Once again, I take this opportunity to welcome the team from FWRM. I shall now give the floor to the representative of the Movement, if they can introduce themselves and we can start with the submission proper.

MS. A. SINGH.- (Inaudible) Justice programme at FWRM. Here with me are my colleagues; Ms. Bernice Lata who is our Legal Rights Officer and we have Ms. Laisa Bulatale, who is our Research Officer.

MR. CHAIRMAN.- Thank you for that introduction and now the floor is all yours to do the submission before the Committee.

MS. A. SINGH.- Thank you, Mr. Chairman. We take this opportunity to present our submission and we will get right into it.

Mr. Chairman, the FWRM was established in 1986. It is a multiethnic and multicultural Non-Governmental Organisation (NGO) committed to removing all forms of discrimination against women through institutional reform and attitudinal change, through targeted research and advocacy. Being a feminist organisation, FWRM uses feminist analysis as a basis for this submission to address inequality.

Global developments in Information and Communication Technologies (ICTs), has meant the increasing number of online users, sharing of personal information online, and the availability of surveillance systems and mass data collection capabilities for both, large companies and Government.

The right to privacy from increased Government surveillance and mass Government data collection in Fiji remains an unexplored territory. In 2015, allegations of neighbouring countries spying on Fiji surfaced in mainstream media, which sparked a national debate on privacy laws and protection of Pacific Island Countries from international surveillance. The impacts of such invasion of privacy on women, children and the vulnerable remain unclear and undocumented.

FWRM takes this opportunity to submit herein our analysis and recommendations in response to the proposed Cybercrime Bill 2020 (Bill No. 11 of 2020).

In terms of the issues of concerns, Ms. Bernice Lata will be discussing the guiding principles to include human rights and freedom.

Moving forward, Ms. Laisa Bulatale will be discussing issue two and I will conclude by discussing Issue No. 3 and the recommendation. I now give the opportunity to Ms. Lata to present.

MS. B. LATA.- Thank you, Artika. Here are some issues of concern for the FWRM.

The first issue would be that the guiding principles include human rights and freedom. FWRM welcomes the effort of the State to align with the International Convention on Cybercrime (Budapest Convention). FWRM notes that the Bill seeks to align to the requirements under the Budapest Convention and also introduces new provisions on substantive cybercrime offences, procedural requirements, remedies in relation to cybercrime offences, the collection of electronic evidence and international cooperation for this purpose as set out in the explanatory notes section.

The FWRM makes reference to the preamble of the Budapest Convention and calls specific reference to paragraph 10 of the preamble of the Convention. ……. (inaudible)

MR. CHAIRMAN.- I am facing some technical glitch at the moment.

MR. I. KOMAISAVAI.- Honourable Chairman, if I may assist. The submitters are submitting through their written submission. I think there are certain technical difficulties from their end. We will have them back again.

MS. B. LATA.- I apologise, I will restart from the point that I was previously making.

The FWRM makes reference to the preamble of the Budapest Convention and calls specific reference to paragraph 10 of the preamble of the Budapest Convention which states, and I quote:

> "Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy."

The FWRM strongly believes that the Bill must have guiding principles for the accurate and appropriate application of the same to ensure that there is no compromise of people's fundamental human rights and freedoms which are also enshrined in Fiji's Constitution by virtue of Section 24 of the said Constitution.

Now, I will hand over the submission to my colleague, Ms. Bulatale.

MS. L. BULATALE.- So the next issue FWRM would like to make for the submission is the issue of right to privacy of women and girls in Fiji. As articulated in the introduction, the right to privacy and invasion of privacy is still an unexplored territory but perhaps now, in the context of COVID-19. The FWRM strongly recommends that the right to privacy be a priority for Government as articulated in both, policy and law, as well as in practice.

We believe that the role of Government in national emergencies, pandemics and national security is that the rights and freedom of Fijians are to be protected and safeguarded as enshrined in our Constitution. But we do know that there is a thin line in that as well as the role and responsibility… (inaudible)…

….(inaudible)….in our submission is that the rationale for mass government surveillance and data collection follow a strict guideline that could be articulated in both, policy and law, practice, as well as a strict criteria with adequate oversight in how mass government surveillance and data collection is carried forward.

MS. A. SINGH.- Mr. Chairman, I will be now discussing the third issue which is privacy and security of Fijian women's human rights defenders. The FWRM notes that in Part 5 - Procedural Measures, Section 16 under General Procedural Powers, the Bill states that in application of the same, the Bill has powers to collect evidence in electronic form, not only for offences under this Bill but also any criminal offence under any other written law.

This is concerning, especially for special groups, such as women human rights defenders as in the past, women human rights defenders have been subject to surveillance, harassment and intimidation, whilst they were carrying out their work in advocating for women's human rights. This particular section could be used as a blanket approval to target women human rights defenders, who are vocal in highlighting the violations of women's human rights.

In the fifth review of the Convention on Elimination of all forms of Discrimination against Women, the CEDAW Committee had made reference to the role of women human rights defenders in promoting the implementation of the Convention. This Bill could be used to create a climate of fear for women human rights defenders, as there are no clear defined threshold for surveillance and investigation, and are keen to carry out their work, guaranteeing the freedom of expression, association, assembly and freedom of the press.

In concluding, we would like to present some recommendations as follows:

(1) FWRM strongly recommends that the proposed Cybercrime Bill 2020 include Article 15 of the Budapest Convention as it is integral to the purpose of the Convention, and meet the guiding principle of the proposed Bill; Article 15 of the Conventions provides for Conditions

and safeguards; for Fiji to meet its obligation under Articles 17 and 19 of the International Convention on Civil and Political Rights (ICCPR).

(2) FWRM calls on the Standing Committee to ensure that the Bill is annexed with a set of comprehensive procedural rules for carrying out investigations by State, or any other investigative body; and that the Bill establishes appropriate, readily accessible and un-bureaucratic redress mechanisms for aggrieved persons (including women, girls and women human rights defenders) investigated under this Bill.

(3) FWRM strongly reiterates the need for the Government to also consult with diverse women's groups and women's human rights defenders. Conducting meaningful engagement and collaborative work with women's rights organisations, local women's groups and grassroots organisations in addressing societal and cultural norms that act as barriers for women and girls is needed during national processes in drafting and implementation of new policies and laws.

(4) FWRM strongly recommends that the Fiji Government show that the measures taken to rationalise mass surveillance and data collection is necessary, has a time limit, and is implemented with transparency and adequate oversight by all stakeholders, women's rights organisations, civil society organisations and the public through meaningful engagement.

That is the end of our submission. We would like to welcome any questions or comments on our submission.

MR. CHAIRMAN.- Thank you very much the team from the Fiji Women's Rights Movement for presenting this comprehensive submission to the Committee. I shall now open the floor if Honourable Members have any questions or clarification they would like to seek from FWRM.

HON. DR. S.R. GOVIND.- Mr. Chairman, I would like to thank the presenters for their insight and comprehensive presentation. I have one comment and perhaps, a question.

A lot has been said about protecting the rights of women and children, especially girls. I was just thinking that currently, a lot of personal information, especially by young people, have been posted on social media, so the protection of rights really starts with individuals. What the Fiji Human Rights Association is doing to educate people not to post unnecessary personal comments on social media which puts them at a greater risk of such crimes.

MS. A. SINGH.- Thank you, Honourable Member. As already mentioned, the FWRM is an NGO looking in the area of legislative and policy reform.

In terms of people out there accessing social media, of course, I would like to make reference to our Constitution which says that everyone has the right of freedom of expression and this is not limited to social media as well. Additionally, how one behaves must, of course, be lawful and in a lawful manner.

In terms of the work of FWRM, we are actually working with the young women's groups. We have multiple forums - we have the Fiji Young Women's Forum, Fiji Women's Forum and we also work

with girls between the ages of 10 years to 14 years old, educating them not only about the right to privacy, but also their right to accessing and lawful use of social media.

Although we strongly believe that everyone has the right, of course, we also must not forget that people should not violate anyone else's right in terms of expression on social media, or even violating their rights.

MR. CHAIRMAN.- Thank you. What are some of your suggestions and comments on the protection of rights online, compared to the protection of rights which is a normal practice in life? What do you have to say with regards to rights of expression online and rights to expression of a person?

MS. S. SINGH.- So, generally with or without online, I will just make reference to the Constitution of Fiji. We are all guaranteed the rights, so these rights are not just limited to online, it is equal across the board because, of course, the Constitution is … (inaudible)… online platforms. So, I believe everyone has the equal right in terms of the Constitution …… enshrined …..(inaudible). These rights upon the …(inaudible)….. and, of course, we know comes to limitations, particularly in terms of harmful incidences as well. So, that is what we all need to be mindful of, and not to violate another person's right, but also in terms of other people violating our rights.

(Inaudible)

MR.CHAIRMAN.- I believe we are, again, are facing some technical cliché there.

MS. A. SINGH.- Would you like me to repeat my response, Sir?

MR.CHAIRMAN.- Just the end, I believe we missed on the last few sentences.

MS. A. SINGH.- All right, I will repeat myself . As I was sharing that because our Constitution grants us these rights, it is not just limited to media platforms or in real life, it is all, across the board.

MR. CHAIRMAN.- All right. I think the network is quite bad today.

HON. R.R. SHARMA.- Mr. Chairman, I would like to thank the presenters this morning. I have no further comments, thank you.

MR. CHAIRMAN.- Any final comments from FWRM with regards to today's submission?

MS. A. SINGH.- No, Sir.

MR. CHAIRMAN.- All right. On that note, thank you very much, Madam, and the team from the FWRM, for availing yourselves to do the submission before us. We shall definitely be deliberating further on the submission that you have provided to us and if there is any further clarification or inquiries that need to be made, we will be writing formally to you to get clarification. Thank you very much for today's submission.

The Committee adjourned at 11.43 a.m.