UNODC
United Nations Office on Drugs and Crime

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

JOINT SUBMISSION BY THE UNITED NATIONS OFFICE ON DRUGS AND CRIMES AND THE OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS TO THE STANDING COMMITTEE ON JUSTICE, LAW & HUMAN RIGHTS, PARLIAMENT OF FIJI ON THE CYBERCRIME BILL 2020

I. INTRODUCTION

The Office of the United Nations High Commissioner for Human Rights (OHCHR) and the United Nations Office on Drugs and Crime (UNODC) present to the Standing Committee on Justice, Law and Human Rights their joint submission on the ***Cybercrime Bill 2020*** referred to hereinafter as "the Bill".

OHCHR and UNODC welcome the opportunity to comment and provide technical guidance on the Bill through this written submission and stand ready to provide further advice to the Standing Committee as deemed necessary .

The Bill has been analyzed taking guiding principles and documents into consideration and is generally found to be well-structured. Our submission therefore focuses on making suggestions and comments to address gaps in legislation as related to computer crimes; recommendations geared towards improving the current text of the Bill; and, by ensuring further clarity, if necessary, and offering *de lege ferenda* proposals for purposes of coherence, consistency and comprehensiveness of the legislative framework.

Honourable Chairman, this joint submission also highlights the main concerns arising from the Bill from an international human rights law perspective.

II. GENERAL COMMENTS

Fiji, with a population of over 900,000 people, has more than half of its population using the internet, with the majority being Facebook users. Making the internet safer and

protecting internet users has become integral to the development of new services as well as defining related government policy. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response and recovery from cyber-crime related incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners.

For coordinated action at the national level, it is best to consult with all stakeholders and for them to be provided with an opportunity to provide comments in the drafting process of the legislative framework. The best way to main public support for the measures is for the government to be open and transparent and involve people in making the decisions that affect them. The right to participate in public affairs, protected under article 25 of the International Covenant on Civil and Political Rights (ICCPR), guarantees the right to take part in policy-making at all levels. This includes the right to participate in legislative review processes. States should provide opportunities for public debate and exchanges with civil society on draft legislation, including the possibility to provide comments and opinions to the relevant public authorities.[1] OHCHR notes the challenges faced in ensuring that public consultations were held due to the restrictions imposed following the declaration of a State of Emergency (SOE) and respective restrictions in response to the COVID-19 pandemic. The significant restrictions on the freedom of movement and peaceful assembly, closure of the courts and schools and the restriction of public sector working hours has made effective discussions, awareness raising and related consultations on the Bill a difficult endeavor. However, OHCHR welcomes the fact that the Bill is currently undergoing a meaningful national consultative process as guided by the Parliamentary Committee.

OHCHR encourages the Parliament of Fiji to continue holding nation-wide consultations and ensure that all groups in society are represented and can meaningfully participate in the process and adopt measures to ensure the participation of those that are marginalised or possibly discriminated against.

In the current situation in response to COVID-19, the use of Information and Communication Technologies (ICTs) may assist in overcoming existing challenges imposed by restrictions imposed for public health reasons. However, the use of ICTs should

[1] See Guidelines for states on the effective implementation of the right to participate in public affairs, A/HRC/39/28, adopted by the Human Rights Council through resolution 39/11.

be guided and regulated by a human rights-based approach, to avoid any adverse impact on individuals and groups that are marginalised or possibly discriminated against. Practical guidance on the measures to be taken to ensure public participation decision-making processes, including on the use of ICTs may be found in the Guidelines for states on the effective implementation of the right to participate in public affairs, adopted by the Human Rights Council in 2018 through resolution 39/11.

The development of a cybercrime-related legal framework is an essential part of developing a cybersecurity strategy. This requires, first of all, the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations, cyberbullying and child pornography. The fact that provisions exist in the existing national criminal code that are applicable to similar acts committed outside the network does not mean that they can be applied to acts committed over the internet as well. Therefore, a thorough analysis of current national legislation is vital to identify any possible gaps that may exist. These include reviewing provisions of the following laws to harmonize provisions with this Bill:

a) Online Safety Act 2018;
b) Crimes Act 2009;
c) Telecommunications Act 2008;
d) Copyright Act 1999;
e) Income Tax (Film-Making and Audio-Visual Incentives) Act 2015; and
f) Proceeds of Crime Act 1997.

Apart from substantive criminal law provisions, the law-enforcement agencies need to be provided with the necessary tools to investigate cybercrimes. Such investigations themselves present several challenges. The tools and instruments needed to investigate cybercrimes can be quite different from those used to investigate ordinary crimes. Both UNODC and OHCHR stand ready to provide guidance on this to the Government of Fiji should our technical assistance thereon be deemed useful.

Currently, the Cybercrime Bill is divided into seven parts. Part 1 contains provisions on the usual preliminaries which include interpretation and jurisdiction. Part 2 refers to offences committed against the confidentiality, integrity and availability of computer data and computer systems. Part 3 features computer-related and content-related offences. Part

4 contains provisions dealing with other offences such as identity theft, theft of telecommunication services, disclosure during an investigation and failure to provide assistance. Part 5 outlines procedural measures and Part 6 includes provisions on international cooperation. Finally, Part 7 contains provisions on related regulations.

Guidance and advisory material used in this submission include the following:

a) Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention;
b) The Protocol on Xenophobia and Racism (ETS 189);
c) Draft UNODC Comprehensive Study on Cybercrime (February 2013);[1]
d) UNODC Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children (May 2015);[2]
e) U.N. study on "fraud and the criminal misuse and falsification of identity" (2007).[3]
f) UNODC Model Law on Extradition[4] and the UNODC Model Law on Mutual Assistance in Criminal Matters[5] may also be of relevance on international cooperation aspects covered by the Bill (particularly when checking the complementarities and the interrelationship between this Cybercrime Bill and the Extradition Act of 2003 and the Mutual Assistance in Criminal Matters Act of 1997);
g) United Nations Convention against Transnational Organized Crime;[6] and
h) United Nations Convention against Corruption.[7]

In addition, the UNODC Cybercrime Repository[8] and its database of legislative provisions on cybercrime and electronic evidences are also at the disposal of national authorities for comparative analysis.

---

[1] Available at https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.
[2] Available at http://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.
[3] The full text of the study is available in the UNODC website: https://www.unodc.org/unodc/en/corruption/identity-related-crime.html.
[4] Available at http://www.unodc.org/pdf/model_law_extradition.pdf.
[5] Available at https://www.unodc.org/pdf/legal_advisory/Model%20Law%20on%20MLA%202007.pdf.
[6] http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.
[7] https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf
[8] Available at https://sherloc.unodc.org/cld/v3/cybrepo/.

III. LEGAL FRAMEWORK AND CONCERNS

The term "cybercrime" is used throughout the legislation but there is no definition of cybercrime given in the interpretation section. Most reports, guides or publications on cybercrime begin by defining the terms "computer crime" and "cybercrime". In this context, various approaches have been adopted in recent decades to develop a precise definition for both terms in legislation. Without going into detail at this stage, the term "cybercrime" is narrower than computer-related crimes as it has to involve a computer network. Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems. The term "cybercrime" is used to describe a range of offences including traditional computer crimes, as well as network crimes. For clarity, it is recommended that the term "cybercrime" in the context of the Bill be properly defined and specified under the interpretation section.

The concept of a "reasonable excuse" is used throughout the text. It should be well established either in case or statutory law. If not, an overly broad interpretation of the concept can lead to over-criminalization and human rights violations. The Bill should be amended to delete any potentially ambiguous terms such as "reasonable excuse". It is recommended that there be specificity of the offences included which is the express requirement that the conduct involved is done "without right". The recommended term "without right" reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law.

Provisions on the misuse of devices is not included in the Bill and we recommend that the Bill include the provisions consistent with Article 6 of the Budapest Convention as it relates to source of offences in related parts 2, 3 and 4. We suggest that provisions related to the misuse of devices are established as a separate and independent criminal offence as part of the Bill with the requirement of an intentional commission of specific illegal acts by using

certain devices or accessing data to be misused for the purpose of committing the offences against the confidentiality, the integrity and availability of computer systems or data. As the commission of these offences often requires the possession of means of access ("hacker tools") or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of an illegal market as regards production and distribution thereof. To combat such unlawful situationsmore effectively, the existing criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences in parts 2, 3 and 4.

We also see a need for the government of Fiji to further address in domestic legislation hate speech and online content that could incite racial or religious hatred and that constitute incitement to discrimination, hostility or violence. We are of the opinion that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability. Further, we believe that Fiji's legislation needs to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems and need to secure a full and effective protectionof all human rights without any kind of discrimination. We strongly recommend criminalisation of acts of a racist and xenophobic nature, inciting racial hatred and hate speech committed through computer systems and social media to be included in the Bill to comply with Fiji's obligations under the United Nations International Convention on the Elimination of All Forms of Racial Discrimination. The Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems can provide guidance on the provisions to include in the Bill. In the opinion of "[t]he United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," certain "forms of expression" should be "prohibited by international law," among them are the "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence," and "direct and public incitement to commit genocide".

This prohibition is also enshrined in Article 20(2) of the International Covenant on Civil and Political Rights of 1966 (which Fiji has ratified in August 2018), prohibits "[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence," and Article III(c) of the Convention on the Prevention and Punishment of the Crime of Genocide of 1948 prohibits direct and public incitement to commit genocide. The "Rabat Plan of Action on the prohibition of advocacy of national,

racial or religious hatred that constitutes incitement to discrimination, hostility or violence" [1] clearly distinguishes between various forms of speech: "expression that constitutes a criminal offence; expression that is not criminally punishable, but may justify a civil suit or administrative sanctions; expression that does not give rise to criminal, civil or administrative sanctions, but still raises concern in terms of tolerance, civility and respect for the rights of others".

We also submit that the provisions of the Bill should afford the same rights and limitations consistently to persons online as it does to persons who do not use the internet or computer systems. The United Nations Human Rights Council has repeatedly affirmed that the "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice"[2]). The freedom of expression is viewed as a right that enables and facilitates the enjoyment of other essential economic, social, cultural, civil and political rights, including the right to freedom of peaceful assembly and association, the right to education, and right to participate in cultural life. The United Nations General Assembly also recognized "that the exercise of the right to privacy is [also] important for the realization of the right to freedom of expression and to hold opinions without interference and is one of the foundations of a democratic society" (GA resolution A/RES/68/167).

IV. COMMENTS ON SUBSTANTIVE PROVISIONS OF THE BILL

Part 1: Section 1 and Section 2 are consistent with Article 1 of the Budapest Convention and other international obligations. We recommend criminalizing hate speech and online content that incite racial or religious hatred that constitutes incitement to discrimination, hostility or violence to be included in the Bill. Should the recommendation be accepted, the definition of racist and xenophobic material" can be included under part 1 to mean "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."

---

[1] A/HRC/22/17/Add. 4.

[2] A/HRC/RES/20/8; A/HRC/RES/38/7; see also GA resolution A/RES/68/167 for the same affirmation for the right to privacy.

Part 2, Section 3

The applicability of the Bill extends to the instances where either the victim computer system(s) or compromised data was (merely) lawfully accessed in Fiji at the time of commission of an offence under this Bill. The provision does not require a physical location of the affected computer systems or data in Fiji. The same applies to subsection 2f, which applies to the instance where the service, used in the commission of an offence, is (merely) accessible in Fiji. It can potentially create overbroad and excessive jurisdiction.

Section 3(3) intends to create a mechanism to enable domestic prosecution and relevant judicial proceedings against a person in lieu of extradition when the latter is rejected on the basis of the nationality of the person sought. The provision extends the application of the Bill to nationals of Fiji who cannot be extradited to a requesting State by virtue of section 18(2)(b) of the Fiji Extradition Act 2003. The United Nations Convention against Transnational Organized Crime contains a similar provision (article 15 paragraph 3). The national legislator may consider adopting a wider approach and foresee the same alternative for cases where extradition is denied on any ground other than that of nationality of the person sought (see article 15 paragraph 4 of the United Nations Convention against Transnational Organized Crime).

Part 2, Section 4

For purposes of coherence and consistency of the overall national legislative framework on related matters, and bearing in mind the savings clause of section 4(1)(a) of the Bill *("Unless otherwise provided in this Act or any other written law, nothing in this Act affects— (a) the liability, trial or punishment of a person for an offence under any other written law"*), attention may need to be devoted to the examination of the interrelationship between the following provisions of the draft Cybercrime Bill of 2020 and the Crimes Act of 2009:

a) Section 5 of the draft Cybercrime Bill 2020 (Unauthorized access to computer systems) and section 340 of the Crimes Act 2009 (Serious computer offences);
b) Section 5(4) of the draft Cybercrime Bill 2020 and section 343 of the Crimes Act 2009 (Unauthorised access to, or modification of, restricted data); and

c) Section 7 of the draft Cybercrime Bill 2020 and section 342 of the Crimes Act 2009 (Unauthorised impairment of electronic communication).

The idea is to improve the means to prevent and suppress computer- or computer-related crime by establishing a common minimum standard of relevant offences. This kind of harmonisation alleviates the fight against such crimes on the national and on the international level as well. Correspondence in domestic law may prevent abuses from being shifted to a Party with a previous lower standard.

Part 2, Section 5

The formulation of the provisions requires further clarity. It`s not clear whether the offence in question is the unauthorized access to a computer system or to computer data. The mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction.

The term "access" comprises accessing the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system.

The term "access" also includes accessing another computer system, connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter. The act must also be committed "without right".

In addition to the explanation given above on this particular expression, it means that there is no criminalisation of the access authorised by the owner or other rightful owner of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."

Part 2, Section 6

This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in the 2013 Constitution of Fiji and this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer. In addition to the provisions stated, we submit that the provisions be consistent to other legislation that protects the use of telecommunication services by criminalizing the illegal interception of phone conversations. It should also be conducive to the law enforcement authorities whose surveillance needs to be lawfully authorised in the interests of national security or the detection of offences by investigating authorities.

Part 3, Section 9

The provisions and wordings seem vague and benefit from further clarifications. The words "loss" and "gain" should be further clarified. For example, the significance of a related financial gain/ loss or risk of loss, damage to reputation. We recommend the drafter reconsider the wordings and take cue from Article 7 of the Budapest Convention which states:

> *"... when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible"*

Part 3, Section 10

From the constituent elements of the offence, as described, the conduct of computer-related extortion is evident, but this is not the case with the element of computer-related fraud.

Indeed, article 8 of the Budapest Convention on Cybercrime (criminalization of computer-related fraud) requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit to another but are not carried out with fraudulent or dishonest intent, are not meant to be

included in the offence established by this article. The offence must be committed "without right", and the economic benefit must be obtained without right. Of course, legitimate common commercial practices, which are intended to procure an economic benefit, are not meant to be included in the offence established by this article because they are conducted with right.

The offence ought to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit to another but are not carried out with fraudulent or dishonest intent, are not meant to be included in the offence established by this article.

In the UN study on "fraud and the criminal misuse and falsification of identity" (2007), the general term "identity-related crime" was used to cover all forms of illicit conduct involving identity, including identity theft and identity fraud. The approach followed was to use this descriptive concept as an "umbrella term" to cover all punishable activities having identity as a target or a principal tool. In some contexts, the term "identity abuse" was also used with a similar meaning. The reason for using such generic terms was the diversity in definitional approaches followed in national jurisdictions in that the same conduct designated as "identity theft" in some countries is seen as "identity fraud" in others.

The UN study further specifies that the term "identity theft", in particular, refers to occurrences in which information related to identity (basic identification information/other personal information) is actually taken in a manner analogous to theft or fraud, including theft of tangible documents and intangible information and deceptively persuading individuals to surrender documents or information voluntarily. On the other hand, the term "identity fraud" generally refers to the subsequent use of identification or identity information to commit other crimes or avoid detection and prosecution in some way.

One of the recommendations made by the UN study was that "law-makers need to develop appropriate concepts, definitions and approaches to the criminalization of a broad range of conducts, including identity theft, identity fraud and other identity-related crimes. It is also

critical for most States to ensure consistency with their respective private and public identity systems and with other already established crimes".

Section 11

From an international standpoint, the term "child sexual abuse material" is increasingly being used to replace the term "child pornography". This switch of terminology is based on the argument that sexualized material that depicts or otherwise represents children is indeed a representation, and a form, of child sexual abuse, and should not be described as "pornography". Pornography is a term primarily used for adults engaging in consensual sexual acts distributed (often legally) to the general public for their sexual pleasure. Criticism of this term in relation to children comes from the fact that "pornography" is increasingly normalized and may (inadvertently or not) contribute to diminishing the gravity of, trivializing, or even legitimizing what is actually sexual abuse and/or sexual exploitation of children.

Furthermore, the term "child pornography" risks insinuating that the acts are carried out with the consent of the child and represent legitimate sexual material.[1] Overall the section on "Child Pornography" is overly broad and needs additional clarification. Specifically, looking at Part 3, section 11, it is not clear what "sexually explicit conduct" is and there is no clear definition within the statute.

That may make prosecution and policing of this law difficult. It may be useful to suggest that language be added to the legislation to further explain what is meant by this term, and thus what is criminal conduct. In addition, it is not clear how it will be determined that the image/video is of a child. The legislation lists that a "prominent impression conveyed is that the person shown is a child." Similar to the issue listed above, this may need more description to clarify exactly what is illegal (what ages) and how that will be determined. It is recommended that the term "without right" be used in the provisions as it does not exclude legal defences, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Accordingly, the term "without right" allows a party to take into account fundamental rights, such as freedom of thought, expression and privacy. In addition, a party may provide a defence in respect of conduct related to

[1] See the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, pp. 37-38 (http://luxembourgguidelines.org/).

"pornographic material" having an artistic, medical, scientific or similar merit. The reference to 'without right' could also allow, for example, that a Party may provide that a person is relieved of criminal responsibility if it is established that the person depicted is not a child in the sense of this provision.

Section 11 paragraph (a) "Takes or permits to be taken child pornography" needs clarity and explicitly specified on whether it refers to downloading, viewing, producing or all of them.

Section 11 (5) should allow for the child abuse material to be uploaded to the INTERPOL Child Sexual Abuse Database (ICSE) or any other similar law enforcement database and for specialized officers to work with the seized material for identifying the victims and ensure that the rights of victims are respected.

Lawmakers in Fiji might consider including additional criminalized acts for the protection of children online, such as online grooming, lying to a child online in order to commit child sexual abuse and exploitation, harassment and prohibition of cyberbullying of children.

Part 4

We recommend that the Government of Fiji also considers including ancillary liability of aiding, abetting and its related sanctions in the Bill to be included under this part.

Part 5, Section 17

This section lists "computers" but does not list cell phones, tablets, and other devices. There is no definition within the legislation indicating that the term "computer" includes all of these items. This may be something to consider and expand. In Part 5, s 17(5), the provision describes how copies of the computer and programs should be made available to the user/owner/defendant. We may want to suggest that, although this review should be allowed, there should be limits and procedures in place to limit the spread and redistribution of contraband that may be on the computer or in the computer programs, like child exploitation files.

Part 5, Section 18

The draft Cybercrime Act contains a series of provisions for the authorization of investigative powers used to gather electronic evidence. As highlighted at the thematic discussion on cybercrime held at the 2018 session of the Commission on Crime Prevention and Criminal Justice, an important factor that needs to be taken into account is the compliance with established procedures that safeguard human rights.[1] When assessing the admissibility of electronic evidence, emphasis should be placed on the importance of compliance with the proportionality principle when using special investigative techniques in cybercrime investigations, including the use of undercover agents and remote forensics, especially on the darknet.

The application of general principles of domestic procedural laws and national jurisprudence pertaining to the admissibility of evidence obtained in forensic cryptocurrency investigations is a new challenging area for further consideration and sharing of experiences due to the innovative techniques used in this context.

Article 20, paragraph 1, of the United Nations Convention against Transnational Organized Crime does not require States parties to take such measures as to allow for the admissibility in court of evidence derived from the use of special investigative techniques, as article 50, paragraph 1, of the United Nations Convention against Corruption explicitly does. This is an element which refers to the positive obligation of a State party to have in place laws, regulations and procedures to enable – for the sake of legal certainty, proper administration of justice and human rights protection – the admissibility before a court of evidence resulting from the use of special investigative techniques.

Despite the lack of this element in article 20, paragraph 1, it is vital for drafters of national legislation to consider the issue of whether evidence obtained through, for example, infiltration can be adduced in court, and, if so, whether the undercover agent has to reveal his/her real identity. It is important to balance the interests of justice with the need to ensure a fair trial of the accused.

---

[1] E/CN.15/2018/6, para. 30.

Both the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption are silent on the issue of the legal value of information derived from special investigative techniques. Decisions pertaining to the conditions for using such information as admissible evidence in courts are thus left to the discretion of the State concerned, taking into account the basic principles of its legal system, the legalization and authentication methods prescribed by its law.

Against this background, it is recommended that section 18 of the draft Cybercrime Act provide some general criteria and guidance to facilitate the work of the judicial authorities when judging on the admissibility of electronic evidence brought to the court (proportionality principle, human rights guarantees, due process clauses). Paragraphs 1-2 of article 15 of the Budapest Convention provide, *mutatis mutandis*, inspiration in this direction.

Section 23 and section 24

This section specifies that under the conditions of this act a judge may issue a warrant requiring **a service provider** to collect and record, intercept and provide traffic data. Depending on technical capabilities, law enforcement agencies may be able to conduct real-time traffic data interception and collection so maybe this sections should not restrict this action only to service providers but allow for other competent authorities, under the provisions of this act, to perform real-time collection of traffic data.

Section 25(2)

It may be prudent to identify that the competent authority to perform the functions described in this provision on behalf of the Government of Fiji is the Attorney-General.

Section 26

By virtue of this provision, the offences established in accordance with this Act are deemed extraditable offences under the Extradition Act 2003. 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 2003 may need to be

reconfirmed: *"3(2) In determining whether conduct constitutes an offence, regard may be had to only some of the acts or omissions that make up the conduct".*

Section 28

This provision specifically provides for limitations on the use of information or material, in order to enable the requested party, in cases in which such information or material is considered particularly sensitive, to ensure that its use is limited to that for which assistance is granted, or to ensure that it is not disseminated beyond law enforcement officials of the requesting party. These restrictions provide safeguards that are available for, inter alia, data protection purposes. It is not understood why the Attorney General as opposed to the Minister for Communications will receive requests and we recommend that due to issues of privacy, the information should rest with the line Minister.

***

Thomas Hunecke
Officer-in-Charge
Regional Office for the Pacific
Office of the United Nations High Commissioner for Human Rights

Dated of this Day: 23/06/2020