**CYBERCRIME BILL 2020**

Ashwin Raj, Director HRADC

**Submission to the Parliamentary Standing Committee on Justice, Law and Human Rights**

30 June 2020

The Convention on Cybercrime or the Budapest Convention, on which the Cybercrime Bill 2020 is premised, entered into force in 2004. It is the sole legally binding international multilateral treaty that addresses internet and computer related crime such as infringements of copyright, computer-related fraud, child pornography and violations of network security. The Convention has created the conditions of possibility for not only the criminalization of certain cybercrime conduct and established the procedures for the investigations of such transgressions but also facilitates investigations through coordination between nation-states. It provides the most comprehensive framework for the development of national legislation and safeguards against cybercrime. As enunciated in its preamble, the objective of the Convention is to prioritise “a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation”.

**Core elements of the Bill**

Even though Fiji has not ratified the Budapest Convention, it is imperative to note that the proposed Cybercrime Bill includes the most salient features of the Budapest Convention and aligns to the requirements of the Convention on Cybercrime.

In consonance with the Convention, the Bill introduces offences against the breach of confidentiality, integrity and availability of computer data and computer systems. These include the unauthorised access to computer systems, unauthorised interception of computer data or computer systems, unauthorised acts in relation to computer data and computer systems and unlawful supply or possession of computer system or other device, or computer data. It also introduces other computer related and content related offences such as computer-related forgery, extortion and fraud and child pornography, identify theft, theft of telecommunication services, disclosure during an investigation and the failure to provide assistance.

The Bill also introduces procedural measures and remedies in relation to cybercrime related offences and the protocols governing the collection of electronic evidence and international cooperation.

|  |  |
| --- | --- |
| **CYBERCRIME BILL 2020** | **CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION)** |
| Clause 3 - Application | Article 22 - Jurisdiction |
| Clause 5 - Unauthorised access to computer systems | Article 2 - Illegal access |
| Clause 6 - Unauthorised interception of computer data or computer systems | Article 3 - Illegal interceptions |
| Clause 7 - Unauthorised acts in relation to computer data or computer systems | Article 4 - Data interference |
| Clause 8 - Unlawful supply or possession of computer system or other device, or computer data | Article 6 - Misuse of devices |
| Clause 9 - Computer-related forgery | Article 7- Computer-related forgery |
| Clause 10 - Computer-related extortion and fraud | Article 8 - Computer-related fraud |
| Clause 11 - Child pornography | Article 9 - Offences related to child pornography |
| Clause 12 - Identity theft |  |
| Clause 13 - Theft of telecommunications services | Article 11- Attempt and aiding or abetting |
| Clause 14 – Disclosure during investigation | XXX |
| Clause 15 - Failure to provide assistance | XXX |
| Clause 16 - General procedural powers | Article 14 - Scope of procedural provisions |
| Clause 17 - Search and seizure | XXX |
| Clause 18 - Admissibility of evidence | XXX |
| Clause 19 - Expedited preservation of stored computer data | Article 16 - Expedited preservation of stored computer data |
| Clause 20 - Expedited preservation and partial disclosure of traffic data | Article 17 - Expedited preservation and partial disclosure of traffic data |
| Clause 21- Production order | Article 18 - Production order |
| Clause 22 - Search and seizure of stored computer data | Article 19 - Search and seizure of stored computer data |
| Clause 23 - Real time collection of traffic data | Article 20 - Real time collection of traffic data |
| Clause 24 - Interception of content data | Article 21 - Interception of content data |
| Clause 25 - General principles relating to international cooperation | Article 23 - General principles relating to international co-operation |
| Clause 26 - Extradition | Article 24 - Extradition |
| Clause 27 - Spontaneous information | Article 26 - Spontaneous information |
| Clause 28 - Confidentiality and limitation on use | Article 28 - Confidentiality and limitation on use |
| Clause 29 - Expedited preservation of stored computer data | Article 29 - Expedited preservation of stored computer data |
| Clause 30 - Expedited preservation of stored traffic data | Article 30 - Expedited preservation of stored traffic data |
| Clause 31- Mutual assistance regarding accessing of stored computer data | Article 31 - Mutual assistance regarding accessing of stored computer data |
| Clause 32 - Transborder access to stored computer data with consent or where publicly available | Article 32 - Trans-border access to stored computer data with consent or where publicly available |
| Clause 33 - Mutual assistance regarding the real-time collection of traffic data | Article 33 - Mutual assistance regarding the real-time collection of traffic data |
| Clause 34 - Mutual assistance regarding the interception of content data | Article 34 - Mutual assistance regarding the interception of content data |
| Clause 35 - 24/7 Network | Article 35 - 24/7 Network |

Pursuant to Clause 3(2) of the proposed Cybercrime Bill, the scope of its application includes:

(a) where a person commits an offence under this Act while being present in Fiji;

(b) on board a ship flying the flag of Fiji;

(c) on board an aircraft registered under the laws of Fiji;

(d) where the alleged conduct was committed by a Fijian citizen, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State;

(e) where the computer, computer system, device, computer data or information affected or which was to be affected, by the act which constituted an offence under this Act, was at the material time lawfully accessible in Fiji;

(f) where the service, including any computer storage, or device or computer data or information processing service, used in the commission of an offence under this Act was accessible in Fiji; and

(g) where the loss or damage is caused in Fiji by the commission of an offence under this Act, to the State or to a person in Fiji.

Clause 3(3) further provides that the proposed Bill is also applicable “to an offender present in Fiji when extradition of the person is not possible, solely on the basis of the person’s nationality”.

Clause 4 provides for the savings of certain laws that unless and otherwise expressly provided in the proposed Bill or any other written law, nothing in the proposed Bill affects the liability, trial or punishment of a person for an offence under any other written law. Clause 4 further provides that if a person performs an act which is punishable both under the proposed Bill and any other written law, the person may only be punished under one such applicable written law.

Part 2 of the proposed Bill provides for offences against the confidentiality, integrity and availability of computer data and computer systems and Clause 5 criminalises intentional unauthorised access to computer systems by persons without lawful authority and introduces a penal liability of a fine not exceeding $10,000 or imprisonment for a term not exceeding five years or both for such an offence and in the case of a body corporate, a fine not exceeding $50,000. Clause 5(5) also provides that a person is exempted from prosecution, if he or she is permitted or required by a court of law or under any other written law to obtain information or take possession of any document or thing.

Clause 6 provides for the offence of unauthorised interception of computer data or computer systems and introduces a penal liability of a fine not exceeding $50,000 or imprisonment for a term not exceeding ten years or both for such an offence and in the case of a body corporate, a fine not exceeding $100,000. The clause further defines what constitutes an act of interception that includes listening to, recording or acquiring the substance, meaning or purpose of the computer data. Clause 6(4) also provides that a person is exempted from prosecution, if he or she has the expressed consent of the person who sent the computer data and the intended recipient of the computer data; or is permitted or required by a court of law or under any other written law to obtain information or take possession of any document or thing.

Clause 7 introduces the offence of unauthorised acts in relation to a computer system or computer data in the event, as per 7(1)(b) the person knows that the act is unauthorised when performing the act. It is illegal data interference when a person who, intentionally and without lawful authority or reasonable excuse interferes with computer data owned or managed by another person by damage to, deletion, deterioration, alteration or suppression of the computer data. This provision applies if the person intends to (a) impair the operation of any computer system (b) prevent or hinder access to any computer data held in any computer system (c) impair the operation or the reliability of any such computer data. This provision applies if the person is reckless as to whether the act will amount to deletion, deterioration, alteration and suppression of computer data. The act is unauthorised if the person committing the act does not have the responsibility for the computer system or computer data, is entitled to determine whether the act may be performed and does not have prior written consent to act. Transgression of this provision attracts a penal liability of a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both in the case of individuals and in the case of a body corporate a fine not exceeding $100,000.

Clause 8 introduces the offence of unlawful supply or possession of a computer system or other device, or computer data which entails the intentional manufacturing, sale, procurement for use, importation, distribution or otherwise makes available a computer system or any other device, or computer data or computer program designed or adapted primarily for the purpose of committing an offence under this clause, commits an offence and is liable on conviction to a fine not exceeding $50,00 or imprisonment for a term not exceeding 10 years or both in the case of an individual and a fine not exceeding $100,000 in the case of a body corporate. Pursuant to Clause 8(2) a person who is in possession of any computer data or computer program, or a computer system or any other device designed or adapted primarily for the purpose of committing an offence under this provision with the intention that it be used by the person or another person to commit or facilitates the commission of an offence, commits an offence and is liable on conviction to a fine not exceeding $50,000 or imprisonment for a term not exceeding 7 years or both in the case of an individual and a fine not exceeding $100,000 in the case of a body corporate. Possession of any computer data includes (a) possession of a computer system or computer data storage device that holds or contains the computer data (b) possession of a document in which the computer data is recorded (c) having control of computer data that is in possession of another person.

Clause 9 provides for the offence of computer-related forgery. Any person without lawful authority or reasonable excuse inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intention of obtaining a gain for the person or another person, or causing loss to another person or exposing another person to risk of loss commits an offence and is liable on conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both in the case of an individual or a fine not exceeding $50,000 in the case of a body corporate.

Clause 10 of the Bill relates to the offence of computer-related extortion and fraud. Any person who intentionally without lawful authority or reasonable excuse performs or threatens to perform any act for the purpose of procuring an economic benefit, for himself or herself or another person, or causing loss to another person or exposing another person to risk of loss, including by undertaking to cease or desist from the act, or by undertaking to restore any damage caused as a result of those cats commits an offense and is liable on conviction to a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both in the case of an individual or a fine not exceeding $100,000 in the case of a body corporate.

Clause 11 provides for the offence of child pornography. Clause 11(2) defines “child pornography” as content that depicts, presents or represents–

(a) a child engaged in sexual intercourse or sexually explicit conduct;

(b) a person appearing to be a child in sexual intercourse or sexually explicit conduct;

(c) an image, animation, text material or video of a child engaged in sexual intercourse

or sexually explicit conduct that includes any audio, visual or text material.

Where, pursuant to 11(3)

(a) the impression conveyed by the content is that the person shown is a child; or

(b) the predominant impression conveyed is that the person shown is a child, notwithstanding that the persons physical characteristics are those of an adult

A person commits an offence if he or she intentionally who intentionally (a) takes or permits to be taken child pornography (b) offers, distributes, makes available or shows child pornography;

(c) procures through a computer system and has in his or her possession child pornography for himself or herself or with a view of the content being distributed or shown to any other person or(d) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes such content or intends to do so. An individual on conviction is liable to a fine not exceeding $50,000 or imprisonment of a term for a term not exceeding 15 years or both and in case of a body corporate a fine not exceeding $200,000. In addition to the conviction, a court may order (a) the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence; or (b) that the material subject matter of the offence no longer be stored on and be made available through the computer system, or that the material be deleted.

Clause 12 provides for the offence of identity theft, specifically the unlawful use of a computer system to intentionally transfer, possess or use a means of identification of another person with the intent to commit or to aid or abet in an activity that constitutes a crime, commits an offence and is liable on conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both in the case of an individual and a fine not exceeding $50,000 in the case of a body corporate.

Clause 13 criminalises the use of a computer and intentional transfer, possession or use of the telecommunications services of another person with the intent to commit or to aid and abet, or in connection with any unlawful activity, commits an offence and is liable on conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both in the case of an individual and a fine not exceeding $50,000 in the case of a body corporate.

Clause 14 provides for the offence of disclosure during an investigation, specifically the unlawful disclosure during an investigation where the fact that an order that confidentiality is to be maintained has been made. A person commits an offence and is liable on conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both in the case of an individual and a fine not exceeding $50,000 in the case of a body corporate.

Clause 15 introduces the offence of failure to provide assistance. A person other than a suspect without lawful authority or reasonable excuse fails to provide assistance or assist a person presenting an order under the prosed Bill commits an offence and is liable on conviction to a fine not exceeding not $5,000 or imprisonment for a term not exceeding 2 years or both in the case of an individual and a fine not exceeding $50,000 in the case of a body corporate.

Clause 16 provides for the general procedural powers, specifically that all powers and procedures under the proposed Bill are applicable to and may be exercised with respect to inter alia any criminal offence established in accordance with the proposed Bill and any other criminal offence committed by means of a computer system established under any other written law.

Clause 17 provides for search and seizure powers. A police officer or an authorised person may apply to a judge or magistrate for a warrant to enter a particular location to search and seize inter alia a computer or computer program. In addition, clause 17 provides that a judge or magistrate may issue the warrant, with or without the assistance of an expert if the judge or magistrate is satisfied on the basis of the evidence and information presented, that the sought computer program, computer system, device or computer data may be material as evidence in proving an offence or acquired as a result of an offence. Clause 17 adopts the definition of ‘seize’ from the *Criminal Procedure Act of 2009*.

Clause 18 provides for the admissibility of evidence that in any proceedings related to any offence under any written law, the fact that evidence has been generated, transmitted or seized from, or identified in a search of a computer system must not of itself prevent that evidence from being presented, relied on or admitted. In addition, clause 18 provides that the powers and procedures provided under Part 5 of the Bill are without prejudice to the operation of, or powers granted under any written law, when exercised lawfully by a police officer or other authorized person, or any regulatory authority that by itself does not investigate or prosecute an offence.

Clause 19 of the Bill provides for the expedited preservation of stored computer data. A police officer or other authorised person may issue a written notice to a person to preserve specified computer data by means of a computer system if the police officer or other authorized person is satisfied that (a) the specified computer data is reasonably required for the purpose of a criminal investigation and (b) there is a risk or vulnerability that the specified computer data may be modified, lost, destroyed, or rendered inaccessible. Clause 19 also provides that the notice must specify a timeframe of 90 days for which the specified computer data must be preserved and which may be renewed once, for a further period of 90 days. A person who contravenes this provision of the proposed Bill commits an offence and is liable on conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both in the case of an individual and a fine not exceeding $50,000 in the case of a body corporate.

Clause 20 pertains to expedited preservation and partial disclosure of traffic data. It provides that a police officer or other authorised person may, by written order, require a service provider to preserve specified traffic data for a period of time in an expeditious manner, regardless of whether one or more service providers were involved in the transmission of the communication in question, for the purposes of a criminal investigation. Contravention of this provision of the proposed Bill carries a fine not exceeding $10,000 or imprisonment for a term not exceeding 7 years or both in the case of an individual and a fine not exceeding $100,000 in the case of a body corporate.

Clause 21 provides that a judge or magistrate may order a person in Fiji to submit specified computer data in that person’s possession or control or a service provider offering its services in Fiji to submit subscriber information relating to such services in that service provider’s possession or control, upon application made by a police officer or other authorised person. Clause 21 further provides that in order for an order to be made, the application must demonstrate to the satisfaction of the judge or magistrate that there are reasonable grounds that the specified computer data or subscriber information is in the possession or control of a person in Fiji or a service provider offering services in Fiji or are required or desirable for the purposes of an investigation. A person who contravenes this provision of the proposed Bill commits an offence and is liable on conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding 7 years or both in the case of an individual and a fine not exceeding $50,000 in the case of a body corporate.

Clause 22 pertains to the search and seizure of stored computer data. It provides that a judge may issue a warrant authorising a police office or other authorised person, to inter alia search and seize stored computer data. In order for a judge or magistrate to issue the warrant, the application for the warrant must satisfy the judge or magistrate that there are reasonable grounds that there may be in a specified computer system, for instance, that is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence. Any person who willfully obstructs or misuses the lawful powers under this provision commits an offence and is liable on conviction to a fine not exceeding $5,000 or imprisonment for a term not exceeding 2 years or both in the case of an individual and a fine not exceeding $10,000 in the case of a body corporate. Clause 22 further defines “decrypted information”, “encrypted data” and “unencrypted version”.

Clause 23 relates the real-time collection of traffic data. It provides that a judge or magistrate may issue a warrant requiring a service provider to collect or record traffic data in real-time and provide only the traffic data to an authorised officer for the purposes of a specific criminal investigation. Clause 23 also provides that a judge or magistrate may only issue such a warrant if the application made satisfies the judge or magistrate that reasonable grounds that the traffic data associated with specified communications and related to or connected with a person under investigation is reasonably required. A service provider who contravenes this provision is liable on conviction to a fine not exceeding $100,000.

Clause 24 provides for the interception of content data. A judge or magistrate may issue a warrant requiring a service provider to intercept content and associate traffic data in real-time and provide that content to an authorised officer as soon as reasonably practicable provided that the real-time interception of content data is not ordered for a period beyond 90 days. Clause 24 also provides that a judge or magistrate may only issue such a warrant if satisfied that the interception of content data is related to or connected with a person or premises under investigation for either the prosecution of a serious offence or to give effect to a mutual assistance request. In addition, clause 24 elaborates on the substantive grounds that must be provided in an application for such a warrant by a police officer or other authorised person. Furthermore, as opposed to other warrants issued under this proposed Bill, a judge or magistrate must require a service provider to keep the warrant issued and execution of any power provided under this provision confidential. A service provider who contravenes a warrant issued under this provision commits an offence and is liable on conviction to a fine not exceeding $100,000.

Clause 25 governs the protocols on general principles relating to international cooperation. 25(1) provides that “the Government may cooperate with any foreign government, 24/7 network, foreign agency or international agency for the purposes of investigations or proceedings concerning offences related to computer systems, electronic communication or data or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of a computer system or real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions” of this proposed Bill.

Clause 26 provides that the offences under Parts 2 and 4 of the Bill are considered extraditable offences under the Extradition Act 2003.

Clause 27 of the Bill provides that the Government may, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings or might lead to a request for cooperation by the foreign State. In addition, clause 27 stipulates that before providing such information to a foreign State, the Government may request that the information be kept confidential and used only subject to specified conditions.

Clause 28 provides that where the Mutual Assistance in Criminal Matters Act 1997 is not applicable to a foreign State, the Government may require a foreign State to keep information provided by the Government confidential. In addition, Clause 28 provides that any such request made on behalf of Fiji must be made only by or with the authority of the Attorney-General.

Clause 29 provides that subject to any limitation specified in Part 6 of the Bill, a foreign government, foreign agency or international agency may request the Attorney-General, or the 24/7 network, to obtain the expeditious preservation of data stored by means of a computer system, located within Fiji or control of the Government. Clause 29 also provides that such a request must be in respect of data which the foreign government, foreign agency or international agency intends to submit a request for mutual assistance for the search of similar access of the data. In addition, Clause 29 provides for the items that must be specified in a request for preservation and that upon receiving such a request, the Attorney-General or 24/7 network must take all appropriate measures to facilitate the request accordingly.

Clause 30 pertains to the expedited disclosure of preserved traffic data. It provides that when the investigating agency discovers that a service provider in another State was involved in the transmission of communications during the execution of a request relating to a specified communication, the Attorney-General or 24/7 network must expeditiously disclose to the requesting foreign government, foreign agency or international agency a sufficient amount of traffic data to identify that service provider and the path through which the specified communication was transmitted.

Clause 31 provides for mutual assistance regarding accessing stored computer data. Subject to any limitations specified, a foreign government, foreign agency or international agency may request the investigating agency to order or search or similarly access, seize or similarly secure and disclose data stored by means of a computer system located within Fiji, including data that has been preserved pursuant to Clause 29.

Clause 32 provides for the transborder access to stored computer data with consent or where publicly available. A police officer or other authorised person may subject any applicable provisions of this proposed Bill access publicly available (open source) stored computer data irrespective of where the data is located or access or received, through a computer system in Fiji, stored computer data located in any territory of a state with whom Fiji has an applicable international agreement.

Clause 33 provides for mutual assistance regarding the real-time collection of traffic data. Clause 33 provides that a foreign government, foreign agency or international agency may request the Attorney-General to order or provide assistance in real-time collection of traffic data associated with specified communications in Fiji transmitted by means of a computer system.

Clause 34 provides for the mutual assistance regarding the interception of content data. A foreign government, foreign agency or international agency may request the Attorney General to order or provide assistance in the real-time collection or recording of content data or specified communications transmitted by means of a computer system in Fiji.

Clause 35 of the proposed Bill empowers the Minister responsible for communications to designate a point of contact or ‘24/7 network’, who must be available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Clause 35 also provides that the point of contact must be properly resourced and that the point of contact also has the authority to coordinate and enable access to international mutual assistance under the Bill.

Clause 36 of the proposed Bill empowers the Minister responsible for Communications (‘Minister’) to make regulations to prescribe matters that are required or permitted by the Bill to be prescribed or are necessary or convenient to be prescribed for carrying out or giving effect to the Bill and generally for achieving the purposes of the Bill. Clause 36 of the Bill also empowers the Minister to make regulations prescribing offences and penalties not exceeding, in the case of an individual a fine of $50,000 or imprisonment for a term of 15 years or both, or in the case of a body corporate a fine of $200,000.

**Interpreting Rights and Limitations in the context of the proposed Bill**

It is imperative that a balanced approach is taken between the just aims of cybercrime legislation as enunciated in the preamble of the Budapest Convention and respect for fundamental human rights and freedoms to ensure that the procedural mechanisms of cybercrime laws including its tools and tactics of investigations that enable the interception of communications and electronic surveillance does not unduly restrict or interdict fundamental rights and freedoms. The scourge of cybercrime offenses such as child pornography, fraud, theft of identity and racial and religious vilification underscoring the importance of legislation to protect human rights is equally sutured by the recognition, as did the Human Rights Council in July 2012 that “the same rights that people have offline must also be protected online”.

However, there is little contestation that if not carefully balanced, cybercrime legislations can disproportionately affect human freedom and dignity, freedom of thought and expression, the right to a fair trial and the presumption of innocence, and freedom from self-incrimination, the right to own property and to protect intellectual property and the right to privacy. While international law enables justifiable restrictions to certain human rights to ensure that the exercise of one’s human rights and freedoms does not result in the diminution of the rights and freedoms of others, it is careful in placing the caveat that these restrictions are in pursuit of a legitimate aim, in accordance with written law, necessary and proportionate to the pressing social need that justified their implementation. Therefore, it is imperative that the restrictions placed are in accordance with the rule of law and human rights with little legal ambiguity as serious human rights challenges can arise from the fact that internet content that might be permissible in one country is made available in another where that content might be deemed illegal.

Similarly, while the Bill of Rights provisions of the 2013 Constitution has robust and salutary human rights provisions encapsulating both civil and political rights as well as economic, social and cultural rights which mirror rights and freedoms enunciated under international human rights conventions and treaties, consistent with international human rights law, some rights and freedoms under the Fijian Constitution come with limitations prescribed by law. Examples include limitations to freedom of speech, expression and publication, freedom of assembly and freedom of association on the grounds of national security, public safety, public order, public morality, public health, the right to be free from hate speech and the right of persons injured by inaccurate or offensive media reports to have a correction published on reasonable conditions established by law.

**What are the principles of constitutional interpretation under the Fijian Constitution?**

*3(1) Any persons interpreting or applying this Constitution must promote the spirit, purpose and objects of this Constitution as a whole, and the values that underlie a democratic society based on human dignity, equality and freedom.*

*(2) If a law appears to be inconsistent with a provision of this Constitution, the court must adopt a reasonable interpretation of that law that is consistent with the provisions of this Constitution over an interpretation that is inconsistent with this Constitution.*

7 (1) In addition to complying with section 3, when interpreting and applying this Chapter, a court, tribunal or other authority-

1. *must promote the values that underlie a democratic society based on human dignity, equality and freedom; and*
2. *may, if relevant, consider international law, applicable to the protection of the rights and freedoms in this Chapter.*

*7 (3) A law that limits a right or freedom set out in this Chapter is not invalid solely because the law exceeds the limits imposed by this Chapter if the law is reasonably capable of a more restricted interpretation that does not exceed those limits, and in that case, the law must be construed in accordance with the more restricted interpretation.*

Furthermore, in the application of the Bill of Rights, section 5 of the Fijian Constitution provides that the rights and freedoms set out in the Bill of Rights chapter apply according to their tenor and may be limited by

1. *limitations expressly prescribed, authorised or permitted (whether by or under a written law) in relation to a particular right or freedom in this Chapter;*
2. *limitations prescribed or set out in, or authorised or permitted by, other provisions of this Constitution; or*
3. *limitations which are not expressly set out or authorised (whether by or under a written law) in relation to a particular right or freedom in this Chapter, but which are necessary and are prescribed by a law or provided under a law or authorised or permitted by a law or by actions taken under the authority of a law.*

**What are the values underpinning a democratic society?**

According to the famous language repeatedly invoked by the Strasbourg Court, a “democratic society” is based on pluralism, tolerance, and open-mindedness. An essential element of “democratic” society, according to the Strasbourg Court’s jurisprudence, is the existence of public confidence in public institutions and authorities.

**What is the Oakes test?**

It is the test for the application of rights and limitations that was first formulated by the Canadian Supreme Court.

Two central criteria must be satisfied to establish that a limit to a right is reasonable and justified in a free and democratic society:

* At a minimum, the limitation of a right must relate to a pressing social need in a free and democratic society.
* The authority limiting a right must show that the means are reasonable and justified.

How is this justification determined? This involves a form of proportionality test involving three important components:

1. The measures must be fair and not arbitrary, carefully designed to achieve the objective of limiting a right and rationally connected to that specific objective of limiting the right in question.

2. The means of limiting the right should impair the right in question as little as possible.

3. There must be proportion­ality between the effects of limiting a particular right and the right in question. In other words, the more severe the deleterious effects of limiting a particular right, the more important the objective for limiting that right must be.

**Based on the Oakes test, how do we read rights and limitations?**

* We read rights broadly
* We read limitations narrowly
* We ask if the limitation is provided for under a prescribed law?
* We ask whether the limitation is intended to respond to a legitimate aim?
* We ask if the limitation is proportionate to the aim?

**Application of international law**

* Section 7(b) also provides that when interpreting the Bill of Rights provisions, a court, tribunal or authority may, if relevant, consider international law, applicable to the protection of the rights and freedoms enshrined in the constitution.

Of pertinence to discussions about the proposed Bill are the following constitutional safeguards and international human rights instruments:

**Human Freedom and dignity**

* **Article 1 of the Universal Declaration of Human Rights**

All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

* **Article 10 of the International Covenant on Civil and Political Rights**

All persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person.

**Rights of the Child**

* **Article 24 (1) of International Covenant on Civil and Political Rights of 1966**

Every child shall have, without any discrimination as to race, colour, sex, language, religion, national or social origin, property or birth, the right to such measures of protection as are required by his status as a minor, on the part of his family, society and the State.

* **Article 10(3) of the International Covenant on Economic, Social and Cultural Rights of 1966**

Special measures of protection and assistance should be taken on behalf of all children and young persons without any discrimination for reasons of parentage or other conditions. Children and young persons should be protected from economic and social exploitation. Their employment in work harmful to their morals or health or dangerous to life or likely to hamper their normal development should be punishable by law. States should also set age limits below which the paid employment of child labour should be prohibited and punishable by law.

* **Article 3 of the United Nations Convention on the Rights of a Child of 1989** the best interests of the child shall be a primary consideration:

1. In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.

2. States Parties undertake to ensure the child such protection and care as is necessary for his or her well-being, taking into account the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her, and, to this end, shall take all appropriate legislative and administrative measures.

3. States Parties shall ensure that the institutions, services and facilities responsible for the care or protection of children shall conform with the standards established by competent authorities, particularly in the areas of safety, health, in the number and suitability of their staff, as well as competent supervision.

The European Court on Human Rights has extended this positive obligation to protect vulnerable persons (namely, children) online by stating that countries are required to implement measures that safeguard them from harm through legislation (e.g., see Mouvement Raelien Suisse v. Switzerland , 2012; M.C. v. Bulgaria , 2003; Perrin v. United Kingdom , 2003 ; K.U. v. Finland , 2008).

* **Section 41 of the Fijian Constitution on the rights of the child**

**Right to privacy**

* **Article 12 of the Universal Declaration on Human Rights of 1948**

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

* **Article 8 of the European Convention on Human Rights of 1950**

Right to respect for private and family life:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with then exercise of this right except such as is in accordance with then law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

* **Article 17 of the International Covenant on Civil and Political Rights of 1966**

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

* **Section 24 of the Fijian Constitution on the right to privacy**

**Freedom of thought and expression**

* **Article 19 of the Universal Declaration on Human Rights of 1948**

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

* **Article 10 of the European Convention on Human Rights of 1950**

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

* **Article 19 of International Covenant on Civil and Political Rights of 1966**

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (order public), or of public health or morals.

* **Article 9(2) of the African Charter on Human and Peoples' Rights of 1981**

Every individual shall have the right to express and disseminate his opinions within the law.

* **Section 17 of the Fijian Constitution on Freedom of speech, expression and publication**

**Right to a fair trial, presumption of innocence and freedom from self-incrimination**

* **Article 11 of the Universal Declaration of Human Rights**

1. Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.
2. No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.

* **Article 9 of the International Covenant on Civil and Political Rights**

1. Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law.

2. Anyone who is arrested shall be informed, at the time of arrest, of the reasons for his arrest and shall be promptly informed of any charges against him.

3. Anyone arrested or detained on a criminal charge shall be brought promptly before a judge or other officer authorized by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release. It shall not be the general rule that persons awaiting trial shall be detained in custody, but release may be subject to guarantees to appear for trial, at any other stage of the judicial proceedings, and, should occasion arise, for execution of the judgement.

4. Anyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings before a court, in order that that court may decide without delay on the lawfulness of his detention and order his release if the detention is not lawful.

5. Anyone who has been the victim of unlawful arrest or detention shall have an enforceable right to compensation.

* **Article 14 of the International Covenant on Civil and Political Rights**

1. All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. The press and the public may be excluded from all or part of a trial for reasons of morals, public order (ordre public) or national security in a democratic society, or when the interest of the private lives of the parties so requires, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice; but any judgement rendered in a criminal case or in a suit at law shall be made public except where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children.

2. Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law.

3. In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality: (a) To be informed promptly and in detail in a language which he understands of the nature and cause of the charge against him;

(b) To have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing;

(c) To be tried without undue delay;

(d) To be tried in his presence, and to defend himself in person or through legal assistance of his own choosing; to be informed, if he does not have legal assistance, of this right; and to have legal assistance assigned to him, in any case where the interests of justice so require, and without payment by him in any such case if he does not have sufficient means to pay for it;

(e) To examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(f) To have the free assistance of an interpreter if he cannot understand or speak the language used in court;

(g) Not to be compelled to testify against himself or to confess guilt.

4. In the case of juvenile persons, the procedure shall be such as will take account of their age and the desirability of promoting their rehabilitation. 5. Everyone convicted of a crime shall have the right to his conviction and sentence being reviewed by a higher tribunal according to law.

6. When a person has by a final decision been convicted of a criminal offence and when subsequently his conviction has been reversed or he has been pardoned on the ground that a new or newly discovered fact shows conclusively that there has been a miscarriage of justice, the person who has suffered punishment as a result of such conviction shall be compensated according to law, unless it is proved that the non-disclosure of the unknown fact in time is wholly or partly attributable to him.

7. No one shall be liable to be tried or punished again for an offence for which he has already been finally convicted or acquitted in accordance with the law and penal procedure of each country.

**Freedom from discrimination**

* **Article 2 of the Universal Declaration on Human Rights of 1948**

Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

* **Article 7 of the Universal Declaration on Human Rights of 1948**

All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

* **Article 14 of the European Convention on Human Rights of 1950 on prohibition of discrimination**

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

* **Articles 2(1) of the International Covenant on Civil and Political Rights of 1966**

1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

* **Article 26 of the International Covenant on Civil and Political Rights of 1966**

All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

* **Article 2(2) of the International Covenant on Economic, Social and Cultural Rights of 1966**

The States Parties to the present Covenant undertake to guarantee that the rights enunciated in the present Covenant will be exercised without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

* **Section 26 of the Fijian Constitution on freedom from discrimination**

**RECOMMENDATIONS**

1. In supporting the enactment of this proposed Bill, the Human Rights and Anti-Discrimination Commission recommends that the moral and legal imperatives of this legislation be balanced with the States human rights obligations under the Fijian Constitution and its obligations under international law.
2. That Fiji considers ratification of the Convention on Cybercrime or the Budapest Convention to ensure compliance with normative instruments.
3. Prioritize awareness and advocacy given the profound legal and human rights ramifications of the proposed Bill.
4. Strengthen the capacity of law enforcement agencies and the private sector in addressing the issue of intermediary liability.