



STANDING COMMITTEE ON JUSTICE, LAW AND HUMAN RIGHTS

Review Report on the Cybercrime Bill 2020 (Bill No. 11 of 2020)



**Parliament of the Republic of Fiji
Parliamentary Paper No. 06 of 2021**

FEBRUARY 2021

Published and Printed by the Department of Legislature, Parliament House, SUVA.

TABLE OF CONTENTS

CHAIRPERSON’S FOREWORD	3
Committee Composition AND REMIT	5
1.0 INTRODUCTION	7
1.1 <i>Background.....</i>	7
1.2 <i>Procedure and Program.....</i>	7
1.3 <i>Cybercrime Bill 2020 (Bill No. 11 of 2020).....</i>	8
2.0 COMMITTEE’S DELIBERATION AND ANALYSIS OF THE BILL	8
2.1 <i>Initial Reading of the Bill and Analysis by the Committee.....</i>	8
2.2 <i>Evidence received via written and verbal submissions</i>	9
2.3 <i>Research into other jurisdictions.....</i>	11
2.4 <i>Sustainable development goals/National Development Plan Impact Analysis</i>	13
3.0 OUTCOME OF REVIEW	13
4.0 CONCLUSION	16

CHAIRPERSON'S FOREWORD

As time changes so does most, if not all, aspects of today's society. Today's society is at the cusp of a technology-driven way of life. This has seen numerous benefits for both the public and private sector, however, it has also seen the growth in the numbers of actors who use technology for malicious and destructive intentions or for their selfish gains. Therefore, numerous jurisdictions have endeavoured to put in place mechanisms for addressing the problematic issues that attach to the proliferated impact of technology, especially those through cyber technology.

There are existing legislation in Fiji that address certain aspects of crimes committed through or on computers, however, change in time came with it, changes in technologies that provided new ways of committing cyber-related crimes. Thus, it was identified that the existing legal and regulatory frameworks do not adequately address crimes committed via or have arisen from ever evolving cyber technology.

Therefore, the Fijian Government, has seen fit to introduce a mechanism for addressing these already existent issues and those novel issues arising from cyber-related and computer related offences. The *Cybercrime Bill 2020*, is this vital mechanism introduced by the Fijian Government.

The *Cybercrime Bill* has been introduced into Parliament and has been referred to the Standing Committee on Justice, Law and Human Rights for review.

For the review, the Committee conducted public consultation, by inviting the public to provide written submissions and also allowing for verbal consultations with key stakeholders and interested individuals.

At the initial stage of the review, the Committee noted a few key points, which are follows:

- a) that the Bill aims to prescribe offences and penalties for acts conducted via cyber space and computers, which negatively impacts an individual, corporate body, society and a nation as a whole;
- b) that certain provisions of the Bill is likely to provide excessive authority and power to the authorities (who, in the case of the Bill, are the police and an authorised person authorised by the Commissioner of FICAC) to search and seize computer data and other information for the purpose of an investigation; and
- c) that certain provisions of the Bill are likely to have implications on potential risks to privacy and court related procedures for adducing evidence.

During the later stages of the review, the Committee identified the following salient issues:

- a) that certain words and phrases found in the Bill should be given proper interpretation provisions;
- b) that certain provisions of the Bill may have unintended consequences on those actors that merely try to expose criminal activities;
- c) that the complex nature of cybercrime and its related matters, i.e. that it is a rapidly evolving part of today's society and that it has extraterritorial implications, should be a key basis for the drafting of the provisions of the Bill;

- d) that there are unrealistic expectations on the practicability of implementing the provisions of the Bill;
- e) that certain provisions could potentially pose risks to certain rights of Fijians, which are provided in the Constitution; and
- f) that the Bill lacks coverage on certain acts, which can be considered as cybercrime.

The Committee compared pieces of legislation of other jurisdictions with the proposed law, to gauge the approaches taken by such jurisdictions in addressing cybercrime and noted that internationally, there are varying approaches in addressing the impacts of advancements in information and communication technologies.

Consideration was also given to the impact of the Bill on the sustainable development goals and the national development plan. It was encouraging to note that the provisions of the Bill are drafted with the aim of enabling development, whilst also promoting a safe and secure cyber-environment. Additionally, the objective of the Bill is as such that it applies equally to all persons, irrespective of gender.

The Committee had extensive internal deliberation on the salient issues noted from the review and legal clarifications were sought on these issues. This ensured that the primary objective of the Bill is preserved.

At the conclusion of the review, the Committee acknowledges that there were numerous issues as identified above. The Committee also realises that the Bill will bring about a new law in Fiji. However, at this stage given the novelty of the implications that the Bill would have on the legal and justice system in Fiji and also on the lives of Fijians; enactment of this law would pose an opportunity for great learning.

Additionally, the Bill is designed to enable the implementation of the *Budapest Convention on Cybercrime* and sets out the minimum requirements, which would ensure Fiji's cybercrime regulatory framework is on par with international standards. It should also be noted that the Bill utilises technology-neutral drafting, thus ensuring that this proposed law is flexible enough to keep up with the ever-evolving nature of cyber-technology and its consequences. Therefore to ensure the fruition of these aims, the Committee believes that the Bill is sufficient as it is and that no amendments are needed.

I would like to thank the Honourable Members of the Justice, Law and Human Rights Committee for their deliberations and input; Hon. Alvick Maharaj (Hon. Chairperson), Hon. Dr. Salik Govind, Hon. Ratu Suliano Matanitobua; and Hon. Mosese Bulitavu, with over a decade of legal research and management. I would also like to acknowledge the staff of the Research Unit and Committee Secretariat, the entities who accepted the invitation of the Committee and made themselves available to make submissions and the members of the public for taking an interest in the proceedings of the Committee and Parliament.

I, on behalf of the Committee, through this Report, commend the *Cybercrime Bill 2020* to Parliament.


.....
Hon. Rohit Ritesh Sharma
Deputy Chairperson

COMMITTEE COMPOSITION AND REMIT

The Committee is made up of Members of both the Government and Opposition Members. The Committee is mandated by Parliament Standing Order 109 (2)(f) and 110 (1) to look into matters relating to justice, law and human rights. This mandate has led to the Parliament through a resolution under Standing Order 51 to refer the *Cybercrime Bill 2020* to the Committee. The Members of the Committee are as follows:



Hon. Alvick A. Maharaj (Chairperson)

- *Assistant Minister of Employment, Productivity, Industry Relations, Youth and Sports*
- *Chairperson of Public Accounts Committee*
- *Government Whip*
- *Pharmacist*



Hon. Rohit Sharma (Deputy Chairperson)

- *Former Civil Servant – Education Sector*
- *Deputy Chairperson of the Standing Committee on Justice, Law and Human Rights*
- *Deputy Government Whip*



Hon. Ratu Suliano Matanitobua (Member)

- *Shadow Minister for Youth and Sports*
- *Former State Minister of Fijian Affairs*
- *Former Military Territorial Officer*



Hon. Dr. Salik Govind (Member)

- *Public Health Specialist – United Nations (World Health Organisation)*
- *Deputy Chairperson of the Standing Committee on Foreign Affairs and Defence Committee*



Hon. Mosese Bilitavu (Member)

- *Shadow Minister for Defense, National Security, Immigration and Correction Services*
- *Former Opposition Whip*
- *Business Consultant/Farmer*
- *Territorial Military Officer – Republic of Fiji Military Forces*
- *Law Graduate and Researcher*

Committee Secretariat Team

Supporting the Committee in its work is a group of dedicated Parliament Officers who make-up the Committee Secretariat, and are appointed and delegated by the Secretary-General to Parliament pursuant to Standing Order 15 (3)(i). The Secretariat team is made of the following Parliament officers:

- Mr. Ira Komaisavai – Senior Committee Clerk
- Mr. Jackson Cakacaka – Deputy Committee Clerk
- Ms. Darolin Vinisha – Committee Assistant

1.0 INTRODUCTION

1.1 *Background*

The Standing Committee on Justice, Law and Human Rights, hereinafter referred to as the Committee, was referred the *Cybercrime Bill 2020* for review on 27 May 2020. The Bill was referred to the Committee pursuant to Standing Order 51 of the Standing Orders of the Parliament of Fiji, whereby the Committee was tasked with scrutinising the Bill and to report back on the Bill in a subsequent Parliament Sitting.

1.2 *Procedure and Program*

i.) Initial Reading of the Bill

The Committee commenced its review by reading through the Bill and conducting its own deliberation of the Clauses in the Bill. An in-depth deliberation of the Bill was conducted by the Committee, whereby pertinent issues were identified.

ii.) Public consultation (written submissions and verbal submissions)

The Committee is also committed to upholding public trust in Parliament, by ensuring that there is public participation and that all such participation is given due consideration. The Committee called for written submissions from the public and other interested stakeholders by placing an advertisement through the Parliament website and social media platforms (Facebook and Twitter).

The Committee received numerous written submissions on the Bill from relevant stakeholders. A summary of these submissions is provided in a later part of this report, under the heading '*Committee's Deliberation and Analysis of the Bill*' and copies of the written submissions can be obtained from the online Appendices of this report, which can be accessed from the Parliament website: www.parliament.gov.fj.

The Committee was mindful of the provisions in Standing Order 111(1)(a) and ensured that its meetings were open to the public and the media, except during such deliberations and discussions to develop and finalise the Committee's observations and this Report. However, it should be worth noting that during the review of the Bill, Fiji like most countries in the world, was not spared from the effects of the global pandemic, Covid-19 (virus). Therefore in order to meet both, the need for curbing the spread of the virus and the requirements of the Standing Orders, the Committee held public consultations via virtual meeting tools.

These virtual meeting tools ensured that Parliament effectively contributed to the efforts of curbing the spread of Covid-19 while still being able to ensure the continuity of the work of Parliament and its Committees.

For this review, the Committee utilised the Microsoft Office Teams computer application, which enabled the Members to hold meetings virtually as a Committee and also for public consultation purposes. All the verbal submissions conducted during the public consultation were also aired Live on the Parliament Channel through the Walesi Platform.

iii.) Legal clarification

To maintain due diligence, the Committee also relies on legal clarification on technical issues identified from the Bill, which is obtained from the Office of the Solicitor-General. These clarifications also assist the Committee in deliberating on these pertinent issues and in deciding whether there will be recommendations for any changes to the Bill.

1.3 *Cybercrime Bill 2020* (Bill No. 11 of 2020)

Fiji, like any other nation in today's world, is not immune to this fast growing trend, thus it is encouraging to note how the Government of Fiji has taken this brave step towards meeting this trend head on.

The introduction of the *Cybercrime Bill* is one such step, albeit, the first; it is a very big step towards ensuring that cyber technology is utilised as it should, but at the same time it does not impede Fiji's efforts towards social, economic and political development.

The *Cybercrime Bill* aims to provide a mechanism to curb the negative impact that attaches to the heavy reliance on cyber related means of doing things.

2.0 COMMITTEE'S DELIBERATION AND ANALYSIS OF THE BILL

2.1 *Initial Reading of the Bill and Analysis by the Committee*

The Committee commenced its analysis of the Bill, reading through it, Clause by Clause. From this initial reading, it was noted that the Bill focuses on introducing criminal offences for such acts that are committed via cyberspace or through a computer.

The Committee had extensive discussions on the provisions of the Bill and identified certain Clauses that merit more deliberation.

These discussions resulted in the identification of a few issues, which the Committee placed as priority issues to be further discussed and deliberated on. Some of the main issues noted from these discussions are as follows:

- the Bill aims to prescribe offences and penalties for acts conducted via cyber space and computers, which negatively impacts an individual, corporate body, society and a nation as a whole;
- that certain provisions of the Bill is likely to provide excessive authority and power to the authorities (who in the case of the Bill are the police and an authorised person authorised by the Commissioner of the FICAC) to search and seize computer data and other information for the purpose of an investigation;
- that certain provisions of the Bill is likely to have implications on potential risks to privacy and court related procedures for adducing evidence.

2.2 Evidence received via written and verbal submissions

All the submissions received were considered and deliberated on extensively. The main points and issues noted from the submissions are summarised below.

Submissions received provided a range of comments and suggestions, which cover various issues pertaining to the Clauses of the Bill.

There were submissions that put forward concerns regarding definitions on certain words and phrases used in the Bill. These words and phrases include, “authorised person”, “person”, “cybercrime”, “Minister”, “reasonable excuse”, “Service Provider”, “Traffic data”, and “loss” and “gains”. There were various arguments on these words, which include that certain words or phrases should be provided clear and concise definitions, or that certain words or phrases be given a broader definition or that certain words or phrases be given definitions or deleted from the Bill.

There were concerns raised that the certain provisions in the Bill, specifically Clauses 5, 6 and 7 which makes unauthorised access, interception and acts, an offence under the Bill. These provisions should also provide for the purpose of the access. It is possible for a person to gain unauthorised access into a system for the sole purpose of finding out information which is not used for any criminal purposes. This is the reason it is important to include a definition of cybercrime because the access must be tied to the purpose of committing a cybercrime.

There is also the likely unintended consequences of the current wording of the provisions. For example, a whistle-blower who gains unauthorised access to his company’s system for the purposes of whistle blowing criminal activities of company is caught under s.5, 6 and 7 even though his intention was not to commit a crime but to expose a crime. It was also submitted that that it is possible to have authorised access and commit a cybercrime using that access. The provisions must provide certainty as to its application so it is not used by police or prosecuting agencies of government for a fishing expedition which can ruin a person’s reputation.

Certain submissions noted the transborder nature of cyber-attacks, which makes it harder to track and investigate. It was submitted that the Bill should not be restricted to Fiji’s jurisdiction and that the Bill should allow authorities to have transborder mutual agreements with other jurisdictions for the purpose of effectively implementing the provisions of the Bill.

Certain submitters argued that the Bill in its current form may also create undue prejudice to a person, especially with regards to a persons’ wellbeing. Thus it was recommended that a body corporate who is possessing, dealing, handling any sensitive information and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or gain to any person shall be guilty of an offence.

Submitters also raised a concern that certain provisions are unlikely to be practicable in Fiji at the current time. Clauses 14, 22 and 23 requires a service provider to perform certain functions that would be difficult to perform at this time. This is because neither

services providers nor enforcement agencies currently have the resources or technical capability to carry out such functions.

Submitters noted that certain provisions of the Bill could potentially infringe on certain rights provided under the *Constitution*. When it comes to investigating a potential cybercrime, the Bill lacks guidance to the Court on what perimeters or the minimum requirements the police or an authorised officer must present to the Court when applying for warrants. This would be problematic in terms of clarity and there is potential for abuse of the warrant for search and seizure of legal and lawful confidential information or personal information or data that does not relate in any way to an investigation.

There was also submission that noted that there is a need to balance the interests of justice with the need to ensure a fair trial of the accused. The Bill provides that gathering of evidence or information derived from special investigative techniques would be sanctioned, however, this is concerning given that the Bill as it is currently drafted is not clear whether it provides sufficient protection against arbitrary interference with the right provided in the *Constitution of Fiji*, section 7(1)(b) and section 24.

There was also concern raised regarding the Procedural Measures provided in the Bill. The Bill provides for procedures for collecting of evidence for the purpose of investigating a cybercrime. However there are concerns raised regarding the applicability of such procedures concerning special groups such as women human rights defenders. There have been instances in the past, where 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. Provisions in the Bill 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 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.

The right to privacy of Fijian women and girls from mass government surveillance and data collection, more so in the context of COVID-19 must be a priority. The right to privacy from government surveillance and mass data collection in Fiji is an unexplored territory, until now. The role of government during a national emergency, disaster or pandemic like COVID-19 is to protect the rights and freedoms of its citizens enshrined under the Constitution. The rationale of increasing government surveillance and mass data collection will be unlawful and intrusive on women and girls' right to privacy unless the government follows strict criteria that is transparent. 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.

Submission also noted that there are strong recommendations that the Fijian 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.

The search scope is unusually relevant in the field of digital evidence and digital forensics. Warrants are crafted around the simple realities of the physical world. The warrant sets down the exact scope of the allowable investigations and any evidence outside the scope is not admissible. There must be a balance in human rights and the responsibility of national security when providing additional powers that could infringe human rights.

Furthermore, there were also submissions that there is a need for expanding the Bill to include provisions that caters for certain activities that are cyber-related, which include:

- a) provisions on cyber-terrorism;
- b) provisions on hate speech, which is politically motivated and cause resentment through social media and other cyber-related mediums;
- c) provisions on communal antagonism, which is line with provisions of the Crimes Act; and
- d) provisions on cyber vandalism;
- e) provisions on Obtaining National Security Information;
- f) provisions on Knowing Transmission and Intentional Damage;
- g) provisions on Intentional Access and Reckless Damage;
- h) provisions on Intentional Access and Damage;
- i) provisions on Trafficking in Passwords; and
- j) provisions on Extortion Involving Threats to Damage Computer.

Transcripts of the submissions can be obtained from the Appendices of this Report, which can be accessed via the parliament website: www.parliament.gov.fj.

2.3 Research into other jurisdictions

In reviewing the Bill the Committee was also conscious of its impact on all the lives of the people of Fiji and noted how the proposed law is a first of its kind for country. Therefore, the Committee believed that it would be prudent to consider looking into other jurisdictions with similar legislation.

The focus of the jurisdictional research was on the approach taken by other jurisdictions that are similar to Fiji regarding cybercrime and also to gauge how the international community have addressed cybercrime.

Firstly, the Committee felt it appropriate to commence its review with various small island developing states in the Pacific region to gauge how the countries dealt with cybercrime. For this part of the review, the Committee relied on publicly available resources, utilising information easily accessible from the internet. These small island developing states in the Pacific region, include Cook Islands, Fiji, Federated State of Micronesia, Kiribati, Nauru, Niue, Palau, Pitcairn Islands, Papua New Guinea, Republic of the Marshal Islands, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu. Australia and New Zealand were also key jurisdictions, which the Committee based its jurisdictional research on.

From the first part of the jurisdictional review it was noted that countries have different approaches in addressing cybercrime and related matters. Certain jurisdictions have

relied on enacting specific legal frameworks/legislation, while other jurisdictions have relied on other legislation, which provides for some aspects of cybercrime.

The Committee noted that Australia and Tonga are the only countries, from the list of Pacific Island countries researched, which had stand-alone cybercrime legislation¹. Other countries, including Fiji, have laws providing for other matters and which also provided for some aspects related to cybercrime. Australia also has enacted a legislation that implements and aligns Australia's cybercrime regulatory framework to the *Budapest Convention on Cybercrime*². Few countries are now opting to explore enacting specific cybercrime legislation in order to address the impacts of cyber-technology, which include Fiji, Kiribati and Vanuatu³.

A detailed list of the countries researched and the status of their cybercrime legal frameworks is included in the Appendices to this Report.

In terms of gauging what the international community has done regarding cybercrime; a good starting point is the information provided in a 2015 press release by the United Nations Conference on Trade and Development (UNCTAD), which states that despite the progress made on addressing cyber-related issues, there were still significant gaps in addressing these issues and one of the key component of this gap is the varying cyber-laws in different countries⁴. This revelation demonstrates the need for harmonised cyber-legislation in countries around the world and that Fiji takes cue from this learnings. The *Budapest Convention on Cybercrime* is one such mechanism for enabling the harmonisation of cyber-laws⁵.

Literature also shows the importance of cooperation between countries when it comes to addressing cybercrime, especially for countries in the Pacific. Research has shown that no one country can address the problem of cybercrime; there is a need for concerted effort and harmonised mechanisms being place⁶.

The jurisdictional review demonstrates that there are varying approaches in dealing with the impacts of new information and communication technologies. Pacific Island countries are not immune from the trend of technological advancements and the impacts that attach to such developments. Each country has its own approach, however this gives an opportunity for countries like Fiji to implement an approach that has been tested on an international level, which is to have stand-alone legislation on cybercrime and related matters.

¹ Council of Europe – Country Profiles on Cybercrime - <https://www.coe.int/en/web/octopus/country-wiki> [accessed on 28 January 2021].

² Ibid 1.

³ Ibid 1.

⁴ UNCTAD Press Release - UNCTAD/PRESS/PR/2015/004: “*Global mapping of cyber-laws reveals significant gaps despite progress*”. <https://unctad.org/press-material/global-mapping-cyberlaws-reveals-significant-gaps-despite-progress> [accessed on 28 January 2021].

⁵ Preamble and Explanatory Note to the Budapest Convention on Cybercrime.

⁶ Professor Angelo, A. H., Professor, Faculty of Law, Victoria University of Wellington, New Zealand.

2.4 Sustainable development goals/National Development Plan Impact Analysis

In reviewing the Bill, the Committee was mindful of its impact on Fiji's efforts in achieving the sustainable development goals and the efforts towards its national development plan.

As a starting point, the Committee highlights the objective of the Bill, which is to address cybercrime by establishing a legal framework that prescribes cybercrime offences and its procedural requirements. This objective relates to the ambitious development plan and goal by the Government of Fiji regarding information and communication technology (ICT) and its utilisation and adoption of new and better technology for and enhancing services in Fiji. In order to improve productivity and ensure better service delivery there were plans to improve universal access to information and competitive telecommunication services, which are delivered on a secure platform. This then brings to the forefront the Fijian Government's priority of creating a safe cyber environment, which enables development.

The Committee was also mindful of the requirements of the Standing Orders of Parliament regarding gender, which is also a key goal in the sustainable development goals. The Committee ensured that full consideration will be given to the principle of gender equality so as to ensure all matters are considered with regard to the impact and benefit on both men and women equally. Despite the lack of gender-related information during the review, it is evident from the deliberations on the Clauses of the Bill that it was designed to impact all Fijians, irrespective of gender.

Therefore, the drafting of the *Cybercrime Bill 2020* takes into consideration the implications of information and communication technology on development and that it is designed to impact every person, irrespective of gender.

3.0 OUTCOME OF REVIEW

After extensive deliberation, the following outlines some of the main outcomes of the Committee's deliberation and review.

The Committee weighed all options concerning the numerous issues that had been identified and had extensive discussions on these. Members of the Committee considered the issues with the assistance of the drafting team, so as to ensure that all these relevant issues were appropriately addressed and that the objectives of the Bill were preserved.

In regard to the finding that certain words and phrases found in the Bill should be given proper interpretation provisions; the Committee noted that certain words such as "authorises person", "person", "Minister" and "reasonable excuse" are words whereby its interpretation are provided in the Bill or in a legislation that provides blanket interpretations of words, such as the *Interpretation Act*. Words such as "service provider" and "traffic data" are words that are directly extracted from the Cybercrime Convention. Therefore, the Committee then resolved that the Bill is drafted closely mirroring the provisions of the *Budapest Convention on Cybercrime*, thus it uses

technology-neutral words. This would ensure that the Bill would have the flexibility to match the ever-changing technologies and its consequences.

In regard to the finding that certain provisions of the Bill may have unintended consequences on those actors that merely try to expose criminal activities; the Committee believes that such provisions are carefully worded so that specific acts are considered as offences and that the ultimate interpretation of the law be left to the jurisdiction of the Courts.

In regard to the finding that the complex nature of cybercrime and its related matters, should be a key basis for the drafting of the provisions of the Bill; the Committee believes that the Bill is drafted in such a way that it allows for flexibility in the law, which in turn enables the Bill to address the ever-changing technologies and its consequences.

In regard to the finding that there are unrealistic expectations on the practicability of implementing the provisions of the Bill; the Committee believes that such a finding relates to resource and capabilities of persons or service providers, thus does not necessarily affect the provisions of the Bill. The Committee also feels that provisions relating to resource and capability and the any consequences arising for that should be left to the jurisdiction of the Courts.

In regard to the finding that certain provisions could potentially pose risks to certain rights of Fijians, which are provided in the *Constitution*; the Committee believes that such implications of the Bill should be left to the jurisdiction of the Courts. This would ensure that a trial is conducted without prejudice and biasness and is according to the set rules and procedures of the Courts.

In regard to the finding that the Bill lacks coverage on certain acts, which can be considered as cybercrime; the Committee is of the opinion that such additional provisions be placed on hold for now. This is due to the fact that the Bill is of a technical nature and that there is a need to urgently put in place a law that would allow Fiji's cybercrime regulatory framework to be of international standards.

It should be noted that internationally, there are varying approaches in addressing the impacts of advancements in information and communication technologies. The evolving nature of technologies has led to the transborder nature of information and communication flow. Jurisdictions are no longer safe from persons that use this transborder flow for destructive purposes or selfish gains, thus the need for solutions that addresses this threat that has defies jurisdictions. The Budapest Convention aims to meet this challenge, but also giving due regard to human rights.

Furthermore, research has demonstrated the need for having a harmonising mechanism for addressing cyber-related issues that are consequences of cyber-technology. This gives an opportunity for a country like Fiji to implement an approach that has been tested on an international level, which is to have stand-alone legislation on cybercrime and related matters.

The Bill also takes into consideration the implications of information and communication technology on development and that the Bill it is designed to impact every person,

irrespective of gender. The Government of Fiji has taken a bold step not to leave Fiji vulnerable to the threats posed by evolving nature of the cyber-environment; by putting forth the *Cybercrime Bill*, which is based on the Budapest Convention. This proposed Cybercrime law will enable Fiji to meet the minimum standards, which would ensure the implementation of the international legal instrument (Budapest Convention) and also open up much needed inter-jurisdictional cooperation and support.

4.0 CONCLUSION

After adhering to due process and the requirements of the Standing Orders of Parliament, the Committee in its deliberation and review noted that there was great support for the Bill.

The review highlighted numerous issues on the Bill, which were considered carefully and extensively by the Committee through internal deliberation and then consultations and legal clarifications being sought on the Bill so as to address all the issues raised and to ensure the objectives of the Bill are not affected. All issues highlighted were addressed by the Committee as provided above and at the conclusion of the review, the Committee is of the opinion that the Bill is sufficient as it is and that no amendments are needed.

The Committee through this report commends the *Cybercrime Bill 2020* (Bill No. 11 of 2020) to the Parliament.

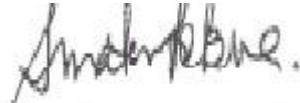
MEMBERS SIGNATURES



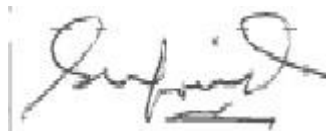
.....
HON. ALVICK MAHARAJ
(CHAIRPERSON)



.....
HON. ROHIT SHARMA
(DEPUTY CHAIRPERSON)



.....
HON. RATU SULIANO
MATANITOBUA
(MEMBER)



.....
HON. DR. SALIK GOVIND
(MEMBER)



.....
HON. MOSESE BULITAVU
(MEMBER)

DATE: 5 February 2021