CONFIDENTIAL

Digicel Fiji (PTE) Limited
Digicel House,
Lot 5 Vuna Road, Nabua
PO Box 13811
Suva
Fiji Islands
www.digicelgroup.com

19 June 2020.

The Chairperson
Standing Committee on Justice, Law and Human Rights
Parliament of the Republic of Fiji
Government Buildings
Suva
Fiji Islands.

Sent via email to : ira.komaisavai@parliament.gov.fj

Dear Chair,

CYBERCRIME BILL 2020 (BILL NO. 11 OF 2020)

We thank the Standing Committee on Justice, Law and Human Rights ("**Committee**") for the opportunity to provide our comments this important piece of legislation.

Digicel (Fiji) Pty Ltd ("**Digicel**") broadly supports Fiji's Cybersecurity initiative. We understand and welcome the approach that has been adopted which is generally consistent with the principles adopted by the *Budapest Convention on of the Council of Europe (CETS No.185)* ("**Budapest Convention**"), an international treaty that is binding on the 65 countries that are parties to it and which serves as an important guideline for any country developing comprehensive national legislation against Cybercrime.

In particular, Digicel recognizes the importance of the introduction of appropriate safeguards that protect ICT infrastructure and the interests of the people of Fiji. Importantly however, those safeguards must strike an appropriate balance between such protections and the rights of individuals and the legitimate commercial interests of providers of ICT services.

In Digicel's respectful view, the Cybercrime Bill, as currently drafted, generally achieves such a balance. However, we believe a small number of important changes are required to:

1. tighten the definition of "service provider" so that it covers all of the key providers of ICT and content related services;

2. make the implementation of the Bill more workable from a practical point of view; and

3. ensure it is consistent with other Fijian legislation.

Each of these issues is dealt with in more detail below.

1. ***Definition of "service provider"***

The *Cybercrime Bill 2020 (Bill No. 11 of 2020)* ("**Bill**") currently defines service provider as follows:

> *""service provider" means—*
>
> *(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or*
>
> *(b) any other entity that processes or stores computer data on behalf of the entity or users of such service provided by the entity;"*

In Digicel's view, there are three issues arising from the particular wording used.

Firstly, as currently drafted, the term "service provider" could apply not only to commercial providers of ICT services but also to private entities or individuals that provide access to their staff or families. This is given the wording in subsection (b) particularly which states "*...entity that processes or stores computer data...*" We do not think that is what the Bill intends and, if left unchanged, would mean that any person who operates a computer system could potentially be considered to be a "service provider". In order to rectify this issue, Digicel proposes it is made clear that the definition of "service provider" is amended so that it refers to any public or private entity that provides services ***to the public***, whether or not such services are provided for direct or indirect financial gain.

Secondly, Digicel is concerned that the definition, as currently drafted, does not clearly capture providers of services on "Over the Top" digital platforms ("**Digital Platforms**") such as online search engines, social media and digital content aggregators like Facebook and Google. This is despite Digital Platforms providing a key mechanism by which cybercrime is committed. In our view, the definition of "service provider" should directly address this by including a third category, being :-

> *"(c) any entity that operates a digital platform providing online search engine, social media, communications and contentment aggregation functions".*

It is important to note that Digital Platform providers encrypt much of their technology and without Fiji being the Regional HUB for these companies as being registered here, they would not have the onus nor impetus to provide decryption to facilitate the provisions under this legislation.

Thirdly, Digicel considers that it is vital that all service providers (as defined above) are registered in Fiji. This is to ensure that service providers are known to the relevant authorities and, in the event that compliance action is required, can be contacted quickly held accountable for their conduct. We propose that such registration is undertaken through the current licensing arrangements that already exist under the ***Telecommunications Act 2008***.

2. *Implementation issues*

Digicel has a number of concerns about the apparently low threshold that has been adopted for interventions under the Bill. For example, sections 18 and 19 of the Bill permit a police officer or other authorized person to issue a notice to preserve specified computer data and traffic information. The threshold for such an order is that "*...the specified computer data is reasonably required for the purpose of a criminal investigation*".

The degree of seriousness of such an offence is not specified and any such order can remain in place for up to 180 days without the police officer or authorised person being required to gain any additional authority for its issuance. In Digicel's respectful view, such orders should only be issued where its is reasonably believed that the investigation is in relation to the investigation of a ***serious*** criminal offence and that any such order should not remain in place for a period of any more than 7 days unless it is authorized by a Judge or Magistrate in accordance with the requirements of section 19(2) of the Bill.

Digicel is also concerned that the threshold for what is considered to be a "serious offence" is set too low in the current draft. At present the threshold is defined to be "*an offence for which the penalty prescribed by law is imprisonment for a term not less than 6 months or a fine not less than $500*". In Digicel's view that threshold is very low and does not reflect the true nature of a "serious offence". It is also likely to mean that service providers will face an unfair burden of providing data and traffic information in respect of offences that are relatively minor in nature. We propose that the definition of "serious offence" be amended so be those criminal offences that carry a maximum prison term of more than 5 years or a fine of more than $10,000.

Finally, Digicel is concerned that the collection and retention of real time computer data and traffic information that is contemplated under sections 22 and 23 of the Bill is unlikely to be reasonably practicable in Fiji at the current time. That is because neither service providers nor law enforcement agencies currently have the resources or technical capability to collect or retain the computer data and traffic information specified in the Bill. Any such future capability would likely require substantial investment that is beyond the limited capacity of domestic service providers, especially in the current difficult economic circumstances that have been brought about as a result of the COVID 19 epidemic.

It is also the case that some computer data, especially that provided or transmitted via Digital Platforms, cannot meaningfully be collected by domestic service providers. This will be expanded upon further in verbal submissions – but the key areas for discussion are threefold with respect to :-

(a) Digital Platform encryption of data so that it cannot be meaningfully collected locally (as above) ;
(b) The ability of users to spoof their IP addresses and/or utilize off the shelf VPN software ; and
(c) the lack of IPv4 internet protocol addresses across the Asia Pacific.

In order to address this important issue, we propose that Fiji adopts there principles set out in the Budapest Convention whereby any compulsion of a service provider to provide real-time traffic data (Art 20) or content data (Art 21) is only to be "...*within its existing technical capability*" [Articles 20 and 21 attached in **Annex** for reference]. Such a provision is especially important in a small country such as Fiji where the resources of both law enforcement agencies as well as service providers are relatively limited and where technical capability and processes may take some time to develop.

Digicel suggests that such a condition could be included with section 14 of the Bill in accordance with the Budapest Convention terminology [Articles 20 and 21 attached in **Annex** for reference] :-

> *"14.–(1) A person, other than a suspect who, without lawful authority or reasonable excuse fails to provide assistance or assist a person presenting an order under this Act, commits an offence and is liable on conviction to—*
>
> *(a) in the case of an individual, a fine not exceeding $5,000 or imprisonment for a term not exceeding 2 years or both; and*
>
> *(b) in the case of a body corporate, a fine not exceeding $50,000.*
>
> *(2) For the purposes of subsection (1), reasonable excuse includes not having the existing technical capability to provide assistance or to assist a person presenting an order under this Act."*

3. ***Consistency with other legislation***

Digicel considers it to be very important that the obligations imposed on service providers under the Bill are consistent with existing obligations under other legislation including the ***Telecommunications Act 2008***.

We are therefore concerned that section 23 of the Bill provides for obligations in respect of the interception of content data when there are similar obligations contained in section 73 of the Telecommunications Act 2008.

We are particularly concerned that subsection 23(6) of the Bill provides a very broad power to compel a service provider to "*...implement the capability to allow interception ..., including specifying the technical requirements and standards for the capability*" but without:

1. making any reference to the terms of on which such an order may be made, including in respect of who will carry the cost of any such implementation; or

2. whether such an order must be reasonable taking into account the existing technical capabilities of the service provider who is the subject of the order.

Relevantly, subsection 74(2) of the ***Telecommunications Act*** provides that :-

> "*...the person must comply with the requirement on the basis that the person neither profits from, nor bears the costs of, giving that help*".

In Digicel's respectful view the retention of this principle is essential to safeguard the legitimate commercial interests of service providers and to protect against regulatory over-reach. This is particularly important at this time given the immense financial pressure that the industry is already under.

We therefore request that a new subsection be added to section 23 of the Bill to confirm that any order to implement the capability to allow interception be made on the basis that:

1. the service provider who is the subject of the order must comply with the requirement on the basis that the service provider neither profits from, nor bears the costs of such compliance; and

2. any technical requirements and standards that are determined by the Minister must take into account the existing technical capabilities of the service provider who is the subject of the order.

Digicel looks forward to the Committee's reasoned consideration of these issues and would be happy to provide any additional detail should that be required.

Sincerely,

.....

Peter Rigamoto
Head of Legal
for **Digicel (Fiji) Pte Limited**

ANNEX :

BUDAPEST CONVENTION ON OF THE COUNCIL OF EUROPE (CETS NO.185)
ARTICLES 21 AND 22.

See in particular blue highlighted area across articles 20 and 21 respectively :-

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

10

ETS 185 – Cybercrime (Convention), 23.XI.2001

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

[redacted]

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.