

28 January 2019

Daw Nwe Ni Soe Yin  
Director, Ministry of Transport and Communications (MoTC)  
By email: [nwenisoeyin@gmail.com](mailto:nwenisoeyin@gmail.com)

Dear Daw Nwe Ni Soe Yin,

**Firstly, we would like to thank the Ministry again for its full participation in the Myanmar Digital Right Forum (MDRF).** There were a number of stakeholders who commented very positively on MoTC's willingness to engage on digital rights. We had 250+ participants in total which demonstrates the growing interest of the Myanmar public in digital rights. We also hope it was helpful to introduce MoTC to new and interested stakeholders. More information on the MDRF is available on our website.<sup>1</sup>

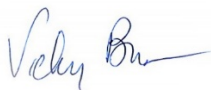
In this letter, we are sending comments as requested during the consultation meeting held on 25 January 2019 on the two reports presented by the consultants TRPC-CMS-Lincoln Legal:

- (1) Legal Advisory of Cyber Legal and Policy Framework: Benchmark Study and Gap Analysis of Cyber Laws - Work Item 5.1 Benchmark Study Against Global Benchmark Indexes
- (2) Legal Advisory of Cyber Legal and Policy Framework: Benchmark Study and Gap Analysis of Cyber Laws - Work Item 5.2 Benchmark Study of Cyber Laws by Jurisdiction

Our brief, overview comments at this stage are set out in the Annex below. We are also taking the opportunity to send soft copies of the Policy Briefs we distributed at the MoTC consultation. In addition, we intend to provide more detailed comments as part of the forthcoming consultations, once the draft policy frameworks(s) and draft law(s) are available for comment.

Thank you again for the opportunity to comment and we look forward in working closely with your Ministry on this important area.

Sincerely,



Vicky Bowman  
Director, Myanmar Centre for Responsible Business

---

## Annex - MCRB Overview Comments

### 1. Consultation Process - Timing

---

<sup>1</sup> <https://www.myanmar-responsiblebusiness.org/news/digital-rights-forum-2019-report.html>

We very much **welcome MoTC's stated intention to hold open consultations** with a wide range of stakeholders on the forthcoming draft policy and legal framework. This is the best way to ensure that MoTC receives and can consider the key concerns of stakeholders before finalising the legislation. It is also an important opportunity for Myanmar stakeholders to be able to participate in policymaking. We encourage you to keep the lines of communication open with stakeholders throughout the drafting and adoption process.

We have already encountered significant interest in the draft legal framework, including in the Pyidaungsu Hluttaw who will need to be **fully briefed** to enable them to play an effective **role as legislators** when drafts are submitted to Parliament.

We believe, however, that the planned **timeframe for adopting such ambitious and important laws is too short**. These are important laws that will shape Myanmar's cyber future and so we would urge the Government to provide for a longer and structured consultation period with stakeholders, to enable them, and government, to become familiar with the issues.

## **2. The Policy and Legal Framework**

As expressed by MCRB and numerous stakeholders at the consultation, we believe that each of the three areas (E-Government, E-Commerce and Cybersecurity) should be **treated in separate laws**. In fact, we think that there should be additional, detailed laws as set out below and in the Policy Brief on the Myanmar Legal Framework (attached).

### **a) New Policies**

We believe it would be very useful to adopt **new policies covering the three areas (E-Government, E-Commerce and Cybersecurity)** that would set out the Government's strategy, its approach and address the measures that do not require laws (e.g. human resource development, developing cybersecurity training, etc).

### **b) New Laws**

We believe that the new cyber legal framework should include the following laws and accompanying regulations (please also see the attached **Policy Brief on the Legal Framework**). As an initial point, we note that each of the laws should include an opening section on objectives. We would like to see clear statements of objectives that include protecting the rights to freedom of expression, assembly, association and privacy in particular.

#### **• Law(s) on E-Government**

- As noted in the consultation, the objective and starting point for E-Government is important for setting the whole approach to E-Government. We would urge as a starting presumption that there should be open access to Government documentation. There will of course be documentation that should not be accessible because of security, privacy, competition, etc. reasons, but we urge an objective of openness.
- We would urge that the E-Government law incorporate requirements on:
  - Data Protection (see below)
  - Open government data
  - A commitment to non-discrimination in access to EGovernment information and services for all
  - And be accompanied by a Right to Information Law
- As to the technical dimensions of what standards should be put in place, we are not experts on E-Government and defer to the technical expertise of the TPRC team on the technical E-Government matters.

#### **• Law(s) on E-Commerce**

- We would urge that the E-Commerce law incorporate requirements on:
  - Data Protection
  - Consumer Protection

- Again, we are not experts on E Commerce and defer to the technical expertise of the TPRC team on the technical matters.
- **Law on Cyber Security**
  - This law should have the objective of protecting individuals, devices and networks while at the same time protecting the freedom of expression and privacy in particular.
  - We would urge that Myanmar direct its limited sources to investing in defensive capabilities to detect and manage threats in order to build trust in business and government services.
  - Please see the attached Policy Briefing on Cyber Security and Cyber Crime for our suggestions on what should be included and what should not.
- **Law on Cyber Crime**
  - Cyber security and cyber crime are different and require distinct approaches. Cyber crime is a criminal law matter and should be treated as a criminal law, not grouped together with cyber security.
  - Please see the attached Policy Briefing on Cyber Security and Cyber Crime for our suggestions on what should be included and what should not.
  - In particular, a cyber crime law should not be used to enhance surveillance, as has occurred in some countries without democratically elected governments such as Vietnam.
  - Any cyber crime provisions should be complemented by human rights safeguards in criminal matters.
- **Law on Data Protection**
  - Data protection is at the heart of all the actions above and is critical to building trust in use of E-Government and E-Commerce systems and facilitating e-connections with other countries.
  - Myanmar has an opportunity to set an example for the region with a data protection law that recognizes privacy rights and has strong accountability mechanisms. The Benchmark Report 5.2 covered the EU's new data protection law,<sup>2</sup> which is rapidly becoming the global standard. Japan and Korea are seeking to demonstrate that their systems are equivalent.<sup>3</sup>
  - For detail, please see our attached our Policy Brief on Data Protection that draws on the EU's GDPR and that sets out what should be covered in a modern, updated data protection law.
- **Law on Lawful Interception**
  - This law should be based on an objective and presumption of protecting freedom of expression while permitting restrictions, monitoring and surveillance only in narrowly defined circumstances as set out in international human rights law for protection of the population.
  - Myanmar needs one consolidated, clear law on lawful interception that incorporates human rights protections. It should clarify, make transparent and restrict the role of the Social Media Monitoring Centre. Please see our attached Recommendations on a rights-respecting lawful interception framework.
  - This should be accompanied by the repeal of existing lawful interception provisions in the Telecoms Law and Narcotics Law.

### c) **Repeal of Existing, Outdated Laws and Contradictory Provisions in Laws**

It was not clear from the consultation whether the consultants have been specifically tasked with making recommendations on amending or repealing existing laws. It will be very important to **repeal contradictory existing laws or sections of existing laws** to ensure that relevant government ministries, companies and other stakeholders have **legal clarity**. Leaving existing, outdated laws in place would cause confusion and undermine the whole purpose of putting new, updated legal framework.

- **Repeal Citizen Privacy and Security Law**

---

<sup>2</sup> The [EU General Data Protection Regulation \(GDPR\)](#)

<sup>3</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en)

- This should be repealed and replaced by an updated and much improved Data Protection Law.
- **Repeal the Electronic Transaction Law & Computer Science Development Law**
  - These are both very outdated and contain vague and harmful provisions and should be repealed and replaced by the new laws.
- **Decriminalize defamation, including through the repeal of Penal Code Section 500; and Telecommunications Law Section 66(d)**
  - Defamation should be treated as a civil liability issue. It should be consolidated into one law, outside the telecoms regulatory framework. MoTC should no longer play a role in this issue.
- **Repeal Sections 40(a), 69, 75 & 77 of the Telecommunications Law & Section 17 of the Narcotics and Psychotropic Substances Law (amended 2018)**
  - These broad and contradictory provisions on lawful interception should be repealed.

### 3. Drawing on Other Existing, More Detailed & Relevant Assessments in Developing Policy and Legal Frameworks

We are aware of the following detailed assessments that have been done on Myanmar's cyber situation, yet we did not see any reference to these in the consultants' reports. The significant analysis and assessment in these documents should be taken into account:

- UNCTAD Myanmar ETrade Readiness Rapid Assessment 2018
- World Bank CyberCrime Capacity Building Assessment of Myanmar 2016
- A cybersecurity assessment by the University of Oxford Global Cybersecurity Capacity Centre

### 4. Comments on Benchmarking Study Work Item 5.1 Benchmark Study Against Global Benchmark Indexes

It is a very interesting and useful study to understand how Myanmar compares and to prepare Myanmar for the 4<sup>th</sup> Industrial Revolution (4IR).

However, we have two overarching comments:

- **Gaps:** The study was (necessarily) selective on the benchmarks chosen. However, the consultants **did not focus on any aspect of digital rights**, such as **surveillance or interception**. This is a significant gap. Numerous international organisations have recognized that protection of human rights must be a core part of cyber policies and laws. See for example the ITU's very recent 2018 guidance for Governments (like Myanmar) on developing a cybersecurity strategy that highlights that human rights should be a core part of the strategy:
  - *"Attention should be paid to freedom of expression, privacy of communications and personal-data protection. In particular, the Strategy should avoid facilitating the practice of arbitrary, unjustified or otherwise unlawful surveillance, interception of communications, or processing of personal data."*<sup>4</sup>
- **Lack of prioritisation:** While the study identifies many gaps, it does not help in prioritizing which should be addressed first. We regret that the whole process of developing the policy and legal frameworks is so rushed and worry that important priorities will be overlooked.
  - MCRB suggests that a **good data protection law should be a top priority**.

We also have a comment on specific sections:

- **Data Protection**
  - Table 1: C1 Privacy and Data Protection is too limited in the issues it covers on data protection. Please see attached our **Policy Briefing on Data Protection**.
  - The **APEC Privacy Framework** falls short of international standards such as the OECD, the EU or the Council of Europe Convention 108 on data protection. The APEC Framework relies excessively on self-regulation and voluntary commitments, which

---

<sup>4</sup> ITU (World Bank and others), [Guide to Developing a National Cybersecurity Strategy](#) (2018)

is not sufficient to regulate company data processing. These other, updated international convention protect people's privacy as a matter of right. That is why countries such as Korea and Japan are working towards being recognised as having an equivalent level of data protection to the EU.

- **Cybersecurity and cybercrime**
    - Again, we think the benchmarking on this area is too limited. In addition, cyber security and cyber crime are not the same and should be treated separately. Please see attached our **Policy Briefing**. We do however, agree with the brief recommendations on cyber crime in the report.
    - In addition, as noted above, the report does not take account of the World Bank assessment of Myanmar on cyber crime.
  
  - **Electronic Authentication**
    - On e-authentication we do not think Myanmar should be moving ahead on digital identification unless the Government:
      - has a data protection law in place that provides robust protection for data gathered by the Government
      - is clear on the objectives and purposes of the developing digital IDs
      - has carefully considered the pros and cons of different systems, considering, for example the serious data breaches that the Indian Aadhaar system has already experienced
      - will provide digital IDs to all on a non-discriminatory basis.
  
  - We **welcome** the coverage of **open government data** and **consumer protection**.
- 5. Comments on Benchmarking Study Work Item 5.2 Benchmark Study of Cyber Laws by Jurisdiction**
- We agree with the overall assessment of the legislative gaps in Myanmar.
  - We re-emphasise that the study had found no other countries with an overall, all-encompassing cyber law as is currently proposed in Myanmar. That is for good reason as each of these areas is complex and should be treated appropriately in specific but coordinated legislation. The study notes that “an omnibus law has many limitations” and that many of the issues can be dealt with through policy or other non-legislative approaches.
  - Hong Kong is considered to be the most forward-looking data protection regime in the region, whereas Singapore has come under consistent criticisms from the digital rights community for its failure to adequately protect privacy.

---

## Attachments

- [MCRB Policy Brief: The Legal and Policy Framework for Information Communication Technology \(ICT\) In Myanmar: Implications For Human Rights](#)
- [MCRB Policy Brief Cyber Security and Cyber Crime: Issues For Myanmar](#)
- [MCRB Policy Brief: A Data Protection Law That Protects Privacy: Issues For Myanmar](#)
- [MCRB Recommendations: A Rights-Respecting Lawful Interception Framework \(see pp. 35-39\)](#)