Myanmar Centre for Responsible Business

# POLICY BRIEF
# THE LEGAL AND POLICY FRAMEWORK FOR INFORMATION COMMUNICATION TECHNOLOGY (ICT) IN MYANMAR: IMPLICATIONS FOR HUMAN RIGHTS

This Policy Brief provides an overview and brief analysis of human rights concerns related to the policy and legal framework that governs Information and Communication Technologies (ICT) in Myanmar. It builds on the Myanmar Centre for Responsible Business (MCRB) "Myanmar ICT Sector Wide Impact Assessment" (SWIA) (published September 2015) that includes a more detailed review of Myanmar's ICT policies and laws.[1]

To implement the type of digital ecosystem necessary for the 4th Industrial Revolution (4IR), Myanmar needs an updated ICT policy and legal framework that is trusted by both users and service providers. Myanmar's current policy and legal framework in the ICT sector is not fit for purpose because:

- There are important gaps in coverage
- The framework is not compatible with changing technology
- Laws do not contain sufficient or appropriate safeguards to protect the rights of privacy and freedom of expression that will encourage users to trust the system

This Policy Brief is intended to support Myanmar in developing a policy and legal framework that will underpin an accessible, inclusive and affordable digital economy[2] that users trust because their human rights are protected.

## RELEVANT MYANMAR POLICIES AND PLANS

The 2016 National League for Democracy's 12 Points Economic Policy[3] highlights the need to develop fundamental economic infrastructure, including several important ICT platforms. To date the following plans have been initiated:

- E-governance Master Plan (2016-2020) (draft)[4]
- Myanmar National Web Portal[5]
- National Data Center[6]

In addition, the Government has developed a draft Universal Service Fund Strategy (2018-2022)[7]. A Digital ID Project is under consideration. A number of other Master Plans exist, but their status is unclear

[1] http://www.myanmar-responsiblebusiness.org/my/swia/ict.html
[2] In line with ASEAN's 2020 ICT Strategy
[3] https://themimu.info/sites/themimu.info/files/documents/Statement_Economic_Policy_Aug2016.pdf
[4] https://www.motc.gov.mm/my/news/myanmar-e-government-master-plan
[5] http://www.mnp.gov.mm/
[6] https://www.mmtimes.com/news/government-build-integrated-data-centre-s-korean-aid.html
[7] https://www.motc.gov.mm/sites/default/files/Universal%20Service%20Strategy%20%28Draft%29_0.pdf

(Myanmar Telecommunications Master Plan) or they have not been renewed (2011-2015 ICT Master Plan). Myanmar is also part of the ASEAN ICT Master Plan 2020.[8]

## RELEVANT MYANMAR LAWS GOVERNING ICT

The most relevant ICT-related laws are:

- Telecommunications Law (2013) (Amended in 2017)[9]
- Electronic Transactions Law (2004) (Amended in 2014)[10]
- Computer Science Development Law (1996)[11]
- Citizens Privacy and Security Protection Law (2017)[12]

These are analysed further below.

## MAIN GAPS IN MYANMAR'S CURRRENT ICT LEGAL FRAMEWORK

Developing an ICT legal framework involves navigating competing demands concerning protection of the rights of people, ICT users, ICT companies and the security of the country's network. For example:

- Intelligence gathering for crime prevention can come into conflict with the right to privacy
- Protecting children online may require certain restrictions on online content

These are not new challenges or unique to Myanmar. Other governments face the same challenges and many are developing legal frameworks that aim to address these issues in a manner that protects human rights and builds trusts among users. That is not yet the case in Myanmar, where there are particular gaps in the legal framework concerning:

- Data Privacy and Data Protection
- Cyber Security
- Cyber crime
- Lawful Interception
- Access to Information
- Intellectual Property

Furthermore, Myanmar's ICT laws have vague or broadly worded provisions that allow the Government and others to use those provisions to threaten and imprison people exercising their rights, particularly to freedom of expression and privacy.

## HUMAN RIGHTS CONCERNS ABOUT MYANMAR'S ICT LAWS

### 1. The 2008 Constitution of the Republic of Myanmar

***Summary of concerns with the Constitution***

- Article 357 of the Constitution provides for a wide scope of protection for communication as it states "*the union shall protect …. correspondence and other communications*". It also provides for the protection of the right to privacy: "*the union shall protect the privacy and security of home, property, correspondence and other communications of citizens.*" However, these protections are subject to vague restrictions: "*subject to the provisions of this Constitution.*" In addition, the protections are available only to citizens.
- The constitutional protections of the right of every citizen to "*express and publish freely their convictions and opinions*" and to freedom of association and assembly (Art. 354) are also restricted

[8] https://www.asean.org/wp-content/uploads/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf
[9] http://freeexpressionmyanmar.org/wp-content/uploads/2017/07/telecommunications-law-en.pdf and http://freeexpressionmyanmar.org/wp-content/uploads/2017/01/Telecommunications-Law-Amendment-EN.pdf
[10] http://freeexpressionmyanmar.org/electronic-transactions-law/
[11] http://www.myanmarconstitutionaltribunal.org.mm/lawdatabase/en/law/1492
[12] http://www.myanmar-responsiblebusiness.org/pdf/Law-Protecting-Privacy-and-Security-of-Citizens_en_unofficial.pdf

by vague references to "*community peace and tranquility*" that go beyond international human rights standards concerning specific conditions that must be satisfied when restricting the exercise of human rights. These protections are also available to citizens only.

- There are no constitutional guarantees of media freedom or access to information in the Constitution.

## 2. Citizens' Privacy and Security Protection Law – 5/2017

The Law Protecting the Privacy and Security of Citizens in March 2017 implements Article 357 of Burma's 2008 Constitution on privacy and security (see above). It is necessary to have a more detailed law on the protection of privacy. However, many of the provisions of the 2017 Law are incompatible with international human rights standards.

***Risks to Privacy and Data Protection***

- The Law contains a vague definition of privacy and a separate definition of security that between them are not in line with international standards on the right to protection of privacy.
- The Law allows for surveillance, interception, entering homes on the basis of permission of a "*Union-level Government body*" rather than only on the basis of a warrant issued by a judge (Art. 8). As there currently is no other law in place on lawful interception, this provides overly broad powers without sufficient safeguards. These safeguards should include judicial oversight of individual requests for telecoms data, clear processes for seeking permission and parliamentary oversight of surveillance.[13]

***Risks to Freedom of Expression***

- Contrary to international norms on defamation that call for civil liability as the appropriate and only form of redress for defamation, Article 8(f) criminalises defamation: "*no one shall act in any way to slander or harm [a citizen's] reputation*". Article 10 imposes a prison sentence and a fine. Criminalising defamation facilitates use of the Law to silence legitimate criticism.[14]

## 3. Telecommunications Law (31/2013 – Amended 26/2017)

The 2013 Telecommunications Law sets out the worthy objectives of providing "support the modernization and development of the nation with telecommunications technology" and to "give more opportunities to the general public to use Telecommunications Services" (Art. 4) but contains a number of overly broad and sweeping powers without appropriate safeguards. The limited 2017 amendments did not address widely expressed concerns with some of these provisions, most notably with Article 66(d), addressed below.

***Risks to the Right to Freedom of Expression:***

- The objectives of the Law do not include protecting freedom of expression (Art. 4)[15]
- ***Criminalization of legitimate online expression***
  - Contrary to international norms on defamation as noted above, the Telecommunications Law criminalises defamation committed via a "*telecommunications network*". (Art 66(d)). This provision has been used repeatedly to restrict the legitimate exercise of freedom of expression and the freedom of the press and to chill freedom of expression.[16]
  - The Law further criminalises additional acts of using a telecommunications network for "*exorting … disturbing or threatening any person*" and for "*communications, reception, transmission,*

[13] Nine Civil Society Organisations Signed A Petition Against the Newly Enacted the Citizens Privacy and Security Protection Bill; Called the Union Parliament and the Government to Review It (March 2017)

[14] Free Expression Myanmar page on defamation

[15] Article 19, "Myanmar Telecommunications Law 2013, (2017)

[16] Between November 2015 and November 2017, 106 complaints were made under this provision, including 13 against journalists. See, *Free Expression Myanmar,* '66(d): No real change', December 2017, http://freeexpressionmyanmar.org/wp-content/uploads/2017/12/66d-no-real-change.pdf. In the first year of the NLD government, 54 cases were initiated under 66(d) compared to seven under the Thein Sein government and although the military was the complainant in several of the cases initiated since the NLD took power, the government has failed to use the veto power over prosecutions that is vested in the Ministry of Transport and Communications under Section 80 of the law. See, *The Irrawaddy,* 'Number Jailed Under Article 66(d) Rises to Eight Since NLD Govt, Htun Htun, 8 April 2017, https://www.irrawaddy.com/news/burma/number-jailed-under-article-66d-rises-to-eight-since-nld-govt.html.

*distribution or conveyance of incorrect information with dishonesty or participation*." These are vague terms that are not defined in the Law or further regulation and can and have been used by the Government to characterise legitimate expression as "*disturbing or threating*", making the expression punishable as a criminal offense. Arts. 66(d) and 68(a).
    - These are "*cognizable offences*", a categorisation that is typically reserved for serious offences such as rape and murder, and that also allow for arrests to be made by a police officer without a warrant issued by a judicial authority (Art 80).
- ***Arbitrary blocking or filtering of content***
    - The Law enables the Ministry, with the approval of the Government, to direct a license holder "*to temporarily suspend a telecommunication service, stop or prohibit any type of communication or use telecommunication services and telecommunication equipment in a temporarily restricted manner when the circumstances warrant for the benefit of the people*." (Art. 77). This is a vaguely worded provision that allows blocking or filtering of content that does not include process or substantive safeguards that would limit the Government's powers to direct a license holder to take these steps.
- ***Arbitrary Disruption or Disconnection of Internet Access***
    - The same provision allows the Government to suspend or take control of telecommunications services, but the situations in which the Government can exercise this power are unclear under the Law (Art. 77).

***Risks to the Right to Privacy***

- ***Government monitoring and surveillance of user activity and content***
    - The Myanmar Government has a long history of close surveillance of its people. The 2013 Telecommunications Law maintains a legal basis for monitoring communications and content. Article 75 allows interception but does not clearly articulate definitions or justifications for interception, beyond a broadly worded reference to "*national security*" and "*rule of law*." Such broadly worded provisions, without further safeguards and more detailed regulations, significantly increase the risk of misuse of intrusive surveillance capabilities. While the clause added that this should be done "*without affecting the fundamental rights of the citizens*," this protection is only available to citizens and raises the question of whether that means that the remaining provisions of the Law are not limited by fundamental rights considerations
- ***Government access to user-identifying information and implications***
    - Article 69 requires a court order for the disclosure of information kept in secured or encrypted systems. However, there are still no implementing regulations governing the interception of communications by law enforcement authorities.
    - The Government has expansive powers to, for example, "*examine any necessary person and require to furnish any necessary information, data, papers and documents*" and to "*enter and inspect*" buildings, places and equipment without any further restrictions. (Art. 40(a)) or "*intercept*" communications when an "*emergency situation*" arises (Art. 77). These powers do not require a court order nor do they need probable cause. Implementing regulations are therefore necessary to provide clarity on the appropriate restrictions and procedures for the exercise of that power.
    - Any or all of the provisions above can be used to override anonymity, and may constitute a separate basis for violation of the right to privacy.

***Implicating Private Sector Companies in Human Rights Violations***

- There is a clear potential for ICT companies to become involved in Government violations of human rights because licensees are subject to suspension or termination of licenses (Art. 5) for failure to comply with a broad set of conditions (Art. 57).

***Extraterritorial Application***

- The Telecommunications Law applies to all Myanmar citizens inside *and* outside the country. This is an extraordinarily broad scope which permits the surveillance of Myanmar citizens as well as other violations of their privacy anywhere in the world.

**4. Computer Science Development Law (CSL) (1996) & the Electronic Transactions Law (ETL) (2004 – Amended in 2014)**

***Risks to Right to Freedom of Expression***

- The Laws include vague and overly-broad criminalisation of expression "*detrimental to security of the State or prevalence of law and order or community peace and tranquility or national solidarity or national economy or national culture, national security and social unity*" (ETL Art. 33(1) & (b) and CSL Art. 35).
- The ETL grants broad powers granted to a "*Control Board*" that is able to access and inspect any ICT it has "*reasonable cause*" to suspect it was used in an offence under the Act (ETL Art. 9 &10.i).

***Risks to Right to Privacy***

- Both laws are outdated and not compatible with current situations and modern technology; there have been numerous calls for their repeal.
- The laws do not provide for data protection, protection of privacy or protection against cyber crime.

***Implicating Private Sector Companies in Human Rights Violations***

- Since Government-issued licenses are required for entities to become a "*certification authority*" for purposes of engaging in electronic transactions, licensees are subject to suspension or cancellation of licenses for failure to comply with Government imposed conditions. This could include requests to turn over information on the identity of users. (ETL Art. 28).

## NEXT STEPS TO BUILD A BETTER ICT LEGAL FRAMEWORK FOR MYANMAR

Myanmar needs to update and revise its ICT framework through consultation with stakeholders, building on past good practice examples of consultations hosted by the Ministry of Transport and Telecommunications.[17] The ICT framework should be based on international human rights and internationally agreed principles and frameworks[18] that incorporate human rights and seek to balance them with the needs of government and users. Steps towards this could include:

- Developing an **ICT strategy** for the country to prepare itself for 4IR that is consistent with international human rights standards
- Establishing a coherent **policy and legal framework** for the ICT sector that involves the repeal or amendment of the existing ICT laws to take account of the concerns highlighted above and includes:
    - Establishing a **cyber security framework,** that includes laws and other approaches
    - Adopting a **separate law or laws which narrowly define cyber crimes** (see MCRB's separate Policy Briefing on Cyber Security and Cyber Crime)
    - Adopting a **Data Protection Law** that protects users' privacy and data online (see MCRB's separate Policy Briefing on Data Protection)**, as a precursor** for **e-government** and **digital ID**
    - Ensuring that the design and implementation of the **e-government** and **digital ID** programmes protects human rights
    - Adopting a rights-respecting **lawful interception framework and laws** based on the seven principles set out in the MCRB ICT SWIA (see Annex to the Recommendations)

[17] See for example the earlier consultation on the Draft Universal Service Strategy.

[18] See for example, the Global Commission on Internet Governance's "One Internet" set of principles (2016).

# Now – Concerns with Current Legal Framework

### 2013 (2017 Amended) Telecommunications Law

- *Criminalizes legitimate online expression using vaguely worded terms (Art. 66(d) and 68(a))*
- *Makes violations of the Law serious offences that allow arrests by the police without without judicial warrants (Art. 80)*
- *Allows government to suspend services,, block or prohibit content and services without safeguards (Art. 77)*
- *Provides vague powers for interception, with limited safeguards (Art. 40(a), 69, 75 & 77)*
- *Potential for license holders to become implicated in violations (Art. 5 & 57)*
- *Law applies to citizens both inside and outside Myanmar*

### 2017 Citizens Privacy and Security Protection Law

- *Has vague definitions of privacy and security not in line with international human rights standards*
- *Permits surveillance, interception, entering homes without judicial warrants (Art. 8)*
- *Criminalises defamation and imposes a prison sentences contrary to international norms that call for civil liability for defamation (Art. 8(f) & 10)*

### 1996 Computer Science Development Law

- *Includes vague and overly-broad criminalization of expression (Art. 35)*
- *Outdated and incompatible with modern technology*
- *Does not provide for data protection, protection of privacy or protection against cyber crime*

### 2014 Electronic Transactions Law

- *Includes vague and overly-broad criminalization of expression (Art. 33(1) & 33(b))*
- *Grants broad powers to access and inspect any ICT (Art. 9 &10.i)*
- *Outdated and incompatible with modern technology*
- *Does not provide for data protection, protection of privacy or protection against cyber crime*
- *Licensees are subject to suspension or cancellation of licenses for failure to comply with Government (Art. 28)*

### 2015 Amendment to the Evidence Act

- *Vaguely defines legitimate electronic evidence and does not make any reference to privacy Sec. 9(g)*

### Penal Code

- *Jail terms for 'offensive' language and defamation (Sec. 124(a))*
- *Violations of freedom of expression (Sec. 505(b) & 505(c))*
- *Prosecution of legitimate journalism (Sec. 500)*

# Future – Improved Legal Framework?

### Repeal the following laws:

- *Citizen Privacy and Security Law*
- *Electronic Transaction Law*
- *Computer Science Development Law*
- *Section 66(d) of Telecommunications Law*
- *Articles in Penal Code Criminalizing Defamation*

### Adopt New Data Protection Law

- *A clear purpose and scope of application based on data protection principles*
- *Protects the rights of data subjects*
- *Limits grounds for processing of personal data*
- *Sets obligations on data controllers and processors*
- *Establish an independent supervisory authority for oversight of data protection*

### Adopt Cyber Security Framework & Law

- *Cyber Security Law*
- *Minimum standards of security, critical infrastructure, incident response team, threat assessments, security audits*

### Adopt Cybercrime Law

- *Incorporate human rights protection and safeguards*
- *Separate cyber dependent and cyber enabled crimes*
- *Define cyber dependent crimes narrowly*
- *Address "cyber enabled crime" through comprehensive criminal laws*

### Adopt Rights-Respecting Lawful Interception Law

- *Do not expand surveillance powers through cyber crime laws*
- *Incorporate rights-respecting provisions to cover both lawful interception and government access to user data (surveillance)*
- *Include appropriate authorisation, oversight, notification of individuals, remedy and transparency*