

Chapter 2

Government Institutions, Policies and Legal Framework



ICT Government Institutions, Policies & Legal Framework

In this Chapter:

- A. Key Actors Regulating Myanmar's ICT Sector**
 - Government Institutions Regulating ICT Operations in Myanmar
 - Other Actors Involved in Myanmar's ICT Sector
- B. Policy Frameworks Guiding Myanmar's ICT Sector**
 - The 2012–2015 Framework for Economic and Social Reform (FESR)
 - The 2011 – 2015 ICT Masterplan
 - The Telecommunications Masterplan
 - The E-Governance Masterplan
 - Regional Policy Frameworks: The 2015 ASEAN ICT Masterplan
- C. International Legal Framework Relevant to Myanmar's ICT Sector**
- D. Domestic Legal Framework Governing Myanmar's ICT Sector**
 - 2013 Telecommunications Law
 - 2004 Electronic Transactions Law
 - 1996 Computer Science Development Law
 - 2014 Law Relating to the Registration of Organisations
 - 1908 Unlawful Associations Act
- E. Guidance for Governments & Companies on Meeting International Standards**

This Chapter sets out the existing Government institutions, policies and legal frameworks relevant to the ICT sector in Myanmar. The absence of clear expectations by Government as to acceptable business conduct, as set out in policies, laws or other expressions of Government expectations, results in gaps that can be filled by responsible – or irresponsible – company actions. As such, impacts often arise from a combination of Government legislation, action or policy (or lack thereof), and company action operating under or outside of the legal and policy framework. It is therefore important to understand whether the policy and legal framework actually requires responsible business conduct, or whether it even addresses relevant issues. It may even actively require businesses to violate international human rights standards in order to comply with national law.

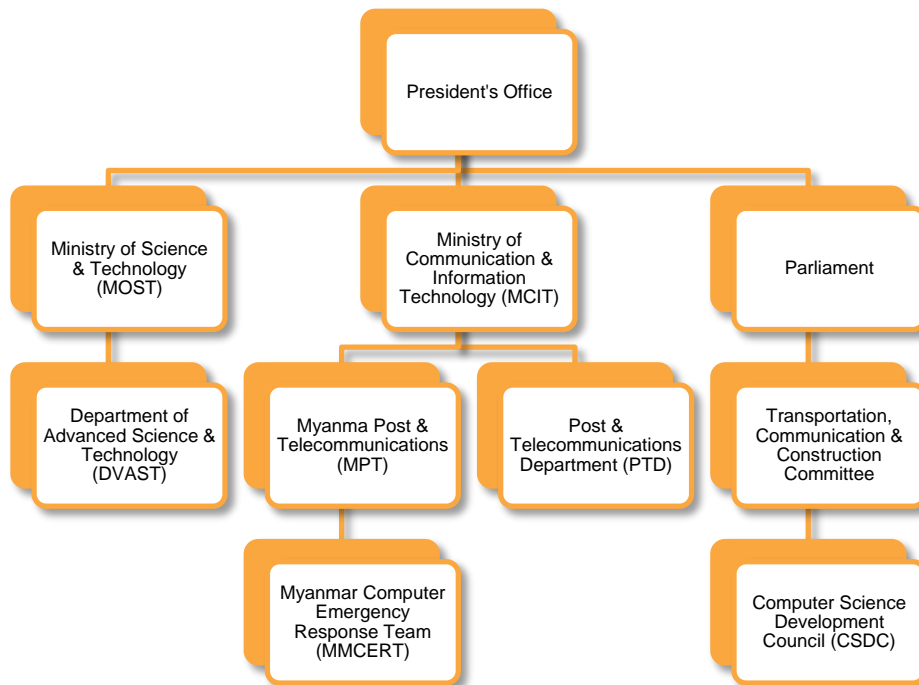
Home governments of international companies operating in Myanmar can also play a role in setting out clear expectations of responsible business conduct.

A. Key Actors Regulating Myanmar's ICT Sector

Government Institutions Regulating ICT Operations in Myanmar

There are a range of Government institutions involved in the governance and regulation of the ICT sector in Myanmar. The main actors and their functions are highlighted below.

Figure 1: Government Institutions Regulating ICT Operations in Myanmar



The Ministry of Communications and Information Technology (MCIT)

The Ministry of Communications and Information Technology (MCIT)⁴⁸ was formerly the Ministry of Posts and Telegrams prior to a restructuring in November 2012. MCIT is the Myanmar Government ministry mandated to guide the development of the country's ICT sector and is the lead ministry responsible for investment in the ICT sector.

MCIT led the 2013-2014 tender process for the licensing of two foreign mobile operators, and has issued the requirements and various classes of licenses available for ICT related businesses (see further [Chapter 3](#), section B on Sector-Level Impacts). MCIT is tasked with modernising Myanmar's ICT sector, supporting on-going liberalisation for local and foreign investors, lowering service prices for customers, developing Myanmar's ICT labour force, and promoting access in underserved locations through the country.

⁴⁸ See the website of the [Myanmar Ministry for Information and Communications Technology \(MCIT\)](#).

Post and Telecommunications Department (PTD) and Myanma Posts and Telecommunications (MPT)

Within MCIT, there are currently two sub-divisions: the Posts and Telecommunications Department (PTD)⁴⁹ and Myanma Posts and Telecommunications (MPT).⁵⁰ Both are currently undergoing wholesale re-structuring. The draft 2015 Telecoms Master Plan outlines a restructure of Myanmar's ICT related institutional framework to create a new 'industry ecosystem'. Under the Master Plan, MCIT will be split into two regulatory bodies and two operators, so that there is independence between operations and regulation, policymaking and oversight responsibilities, including for cybersecurity. Committing to a clear legal, regulatory, and technological separation between Ministry of Communications and Information Technology (MCIT), service operators (MPT and private), and security agencies is a welcome step in the reform of the ICT sector (see further [Chapter 4.3](#) on Privacy and [Chapter 4.4](#) on Surveillance).

PTD is currently the ICT regulatory authority in Myanmar and manages the telecommunications licensing system and spectrum management (detailing specific technology and businesses permitted to transmit on specific radio frequencies in Myanmar). PTD is intended to become an independent regulator⁵¹ by end 2015, to be called the Myanmar Communications Regulatory Commission (MCRC). Its core functions will reportedly be: licensing; spectrum management; interconnection; infrastructure sharing; price and access regulation; equal access and competition; and consumer rights and disputes management. ICT Security (ICTS) will be the other regulatory authority, responsible for e-government, ICT security and satellites, and will incorporate the Myanmar Computer Emergency Response Team (MMCERT), the primary national-level government entity monitoring and reporting cyber-security incidents.

Myanma Post and MPT are the two operators. MPT is a Government-owned mobile network operator and provider of fixed line Internet and voice services. As part of the World Bank's Telecommunications Sector Reform Project, it is undergoing a process of corporatisation. In July 2014 MPT announced a joint operations agreement with Japan's KDDI Summit Global Myanmar Co. Ltd. (KSGM). KSGM is a subsidiary of a joint venture between Japanese telecommunications operator KDDI and Sumitomo Corporation. The joint operations agreement is focused on upgrading existing telecommunications infrastructure, enhancing customer service, and reorganising business processes for MPT⁵².

⁴⁹ Ibid.

⁵⁰ Ibid.

⁵¹ See World Bank "[Project Appraisal Document On a Proposed Credit in the Amount of SDR 20.60 Million \(\\$31.5 Million Equivalent\) to the Republic of the Union of Myanmar for a Telecommunications Sector Reform Project](#)" (January 2014), p3.

⁵² KDDI Corporation, "[Entering the Telecommunications Business in the Republic of the Union of Myanmar](#)" (July 2014).

Ministry of Science and Technology (MOST)

The Ministry of Science and Technology (MOST) is active in ICT human resource development in Myanmar and responsible for the management of technical and computer universities.⁵³ Within MOST, management of computer universities is overseen by the Department of Advanced Science and Technology (DAST). In addition to the 26 computer universities currently in existence in Myanmar, DAST also manages five technological colleges. Yangon Technological University and Mandalay Technological University are designated as “*Centres of Excellence*”. Through a partnership with the Government of India, DAST also manages the India-Myanmar Centre for Enhancement of Information Technology Skills (IMCEITS) located in Yangon.

Computer Science Development Council

The Computer Science Development Council was established in 1996 by the *Computer Science Development Law* (see Section D below). The Council is responsible for developing policies related to information technology, computer networks, and computer science. The Council is chaired by the Union Minister of MCIT and plays a key role in the development of ICT policy, providing legislative inputs to the Pyithu Hluttaw Transportation, Communication and Construction Committee. The Council is comprised of various ministers and members of Government departments or organisations.⁵⁴ Civil society members are not included in the Council’s membership, although it includes members in its Executive Committee from the Myanmar Computer Federations (MCF) (see Table 5 below), as a channel for providing subject matter expertise during the legislative process.

Under the 1996 *Computer Science Development Law* the stated duties of the Council include:⁵⁵

- Setting policy and giving guidance for the “*development of computer science in the State*” and the development of an ICT network
- Supervising and giving guidance with respect to activities of the Federation and other computer-related associations
- Prescribing the types of computer software and information which are not permitted to be imported or exported⁵⁶
- Abolishing any computer association formed or existing or not functioning in conformity with the provisions of the law or the constitution of the relevant association.

Other Actors Involved in Myanmar’s ICT Sector

Other Actors Involved in Myanmar’s ICT Sector

There are a number of other actors and multi-stakeholder bodies relevant to Myanmar’s ICT sector (some of which have been established or supported by the Myanmar

⁵³ See: Modins, “Government and Policy: Ministry of Science and Technology” (last accessed August 2015).

⁵⁴ See the *Myanmar Computer Science Development Law* (No.3/96), section 4.

⁵⁵ Ibid, section 8.

⁵⁶ Ibid.

Government) and include representatives from the private sector, civil society organisations, and key development partners.

Table 5: Other Actors Involved in Myanmar’s ICT Sector

The Myanmar Computer Federation (MCF)

Established in 1998 as part of the *Computer Science Development Law*. MCF is an umbrella organisation made up of all the official computer-related associations and technical groups in Myanmar. The MCF performs a variety of functions including assisting in the development of ICT policy, holding technical seminars and workshops, holding ICT case study competitions, trainings, and sending delegations overseas. The MCF works closely with the Computer Science Development Council. There are various sub-associations of Myanmar Computer Federation, including the Myanmar Computer Industry Association (MCIA), Myanmar Computer Professionals Association (MCPA) and Myanmar Computer Enthusiasts Association (MCEA).

Myanmar Computer Industry Association (MCIA)

The MCIA leads coordination between State and Division level computer industry associations, while working to implement the objectives in the 1996 *Computer Science Development Law*. The MCIA State and Division associations include⁵⁷:

- Yangon Computer Industry Association (Yangon)
- Mandalay Computer Industry Association (Mandalay)
- Ayeyarwaddy Computer Industry Association (Patheingyi)
- Sagaing Computer Industry Association (Monywa)
- Shan Computer Industry Association (Taunggyi)
- Mon Computer Industry Association (Mawlamyine)
- Bago Computer Industry Association (Bago)
- Magway Computer Industry Association (Magway)

Myanmar Computer Professionals Association (MCPA)

The MCPA functions similarly to the MCIA in terms of serving as a coordinating body between State and Division level organisations. The MCPA holds seminars related to computer science and also participates in research related to computer science and technology.

Myanmar Computer Enthusiasts Association (MCEA)

Established in 1998, the MCEA includes over 100,000+ basic education student members.⁵⁸ MCEA does not currently have an independent website.

⁵⁷ See, [Myanmar Computer Industry Association](#), “Organisational Structure” (last accessed August 2015).

⁵⁸ See, Myanmar Computer Federation, “MCEA” (last accessed August 2015).

ICT Sector Working Group

The ICT Sector Working Group is one of the 16 sector working groups established as a result of the Nay Pyi Taw Accord⁵⁹ between the Myanmar Government and donor governments.⁶⁰ The ICT Sector Working Group comprises development partners, the Government, the Myanmar Computer Federation (MCF), Myanmar Development Resources Institute, Myanmar ICT for Development Organisation (MIDO), and the Myanmar Centre for Responsible Business (MCRB).⁶¹

The ICT Sector Working Group was established to support the transformation of Myanmar's ICT sector, with a focus on developing an effective regulatory framework that "*facilitates entry of private service providers*".⁶² Additional focus areas include E-governance, ICT education for all, and improving access to technology for students and workers.

ICT for Development (ICT4D) Working Group

'ICT 4 Development' (ICT4D) is a broad field including but not limited to using ICT to promote mobile health, education and agriculture. The ICT4D Working Group acts a focal point for communication and coordination between stakeholders, while also promoting common platform development and sharing of best practices. Membership in the ICT4D Working Group is open. Current members include NGOs, international donors, private sector companies, civil society organisations. The ICT4D working group is chaired by PACT, a U.S. based international NGO.⁶³

For the main NGOs and CSOs working in the ICT sector see the current list of '[Linked Initiatives](#)' on MCRB's website.

Donor Programmes: The World Bank's Telecommunications Sector Reform Programme

The World Bank's Telecommunications Sector Reform Project with the Ministry of Communications and Information (MCIT) is a \$31.5 million project running from April 2014 to June 2019. The Project's primary goals are to:

- "(a) improve the enabling environment for the telecommunications sector and extend coverage in selected remote pilot locations; and*
- (b) establish priority eGovernment technological foundations institutional capacity for Government to embark on its public sector reform program."*⁶⁴

59 See "Nay Pyi Taw Accord for Effective Development Cooperation" (last accessed August 2015).

60 See, Myanmar Information Management Unit, "Aid Policy and Coordination" for additional information on Government of Myanmar-Development Partner meetings (last accessed August 2015).

61 See: Sector [Working Group Dashboard](#) available from MOHINGA Resources (last accessed August 2015).

62 See "Communication and Information Technology Sector Working Group Dashboard"

63 For additional information on the ICT4D Working Group, please see "Terms of Reference"

64 See World Bank "Project Appraisal Document On a Proposed Credit in the Amount of SDR 20.60 Million (USD 31.5 Million Equivalent) to the Republic of the Union of Myanmar for a Telecommunications Sector Reform Project" (January 2014), pg v.

The primary goal of the ‘enabling environment’ project component is the establishment of competitive sector. To achieve this, the World Bank is providing technical assistance, policy guidance, and assistance in financing key investments such as a spectrum management and monitoring system, which will allow MCIT to designate which entities are permitted to use specific radio frequency for wireless communication and to monitor compliance. \$2.2 million will be allocated to support the corporatisation of MPT and the eventual registration of MPT as a limited liability company.⁶⁵ The World Bank will also be providing “*technical assistance as needed for due diligence reviews of a suite of laws, including privacy, data protection, cyber-crime and access to and freedom of information and recommendations regarding the elaboration of legal and regulatory tools reflecting international best practice in these areas.*”⁶⁶

In order to facilitate increased rural connectivity, the World Bank is supporting MCIT in the development of a process that would subsidise telecommunications and Internet infrastructure in areas of Myanmar that may otherwise be considered economically unviable.

The majority of the ‘enabling e-government foundations’ component will be devoted to developing a ‘Myanmar National Portal’ to provide “*citizens, businesses and visitors (including foreign workers, investors and tourists) with a single on-line window for Government information and services*”.⁶⁷ The portal will reportedly be developed into a mobile friendly tool for users to find such information in the Myanmar and English languages.⁶⁸ The portal will also provide an outlet for users to provide suggestions and feedback about poor service delivery or incidents of corruption, and transact services in a safe and convenient electronic environment. This important objective of improving transparency and accountability represents a significant and welcome shift from earlier Government practices.

While a public consultation with civil society and community members was held in relation to the Telecom Sector Reform Project, it has been the subject of criticism from some civil society groups concerned that human rights considerations, particularly in terms of privacy and surveillance, have not been incorporated into project plans or priorities.⁶⁹ In addition, civil society has drawn attention to the lack of consideration of human rights risks within seemingly ‘neutral’ issues like equipment procurement, expressing concerns about the potential installation of equipment such as deep packet inspection can be used to detect abnormal network activity that may be evidence of a cyber-attack but can also enable the filtering of content and surveillance (see further [Chapter 4.3](#) on Privacy and [Chapter 4.4](#) on Surveillance).

65 Ibid, pg. 8.

66 Ibid, pg. 25.

67 World Bank, “Myanmar Moves Toward Connectivity for All” (6 February 2014).

68 See, World Bank “Project Appraisal Document On a Proposed Credit in the Amount of SDR 20.60 Million (USD 31.5 Million Equivalent) to the Republic of the Union of Myanmar for a Telecommunications Sector Reform Project” (January 2014), pg 21.

69 US Campaign for Burma et al, “[Civil Society Comments on the World Bank Telecom Sector Reform Project in Burma](#)” (21 January 2014).

See Section B below.

B. Policy Frameworks Guiding Myanmar's ICT Sector

The 2012–2015 Framework for Economic and Social Reform (FESR)

President Thein Sein's post-election political, economic and administrative reforms were formalised in the Government's 2012–2015 Framework for Economic and Social Reform (FESR)⁷⁰ which is meant to be a 'reform bridge' linking current reform programmes to the Government's twenty-year national development plan. The FESR identifies priority sectors and potential 'quick wins', is meant to serve as a reference in developing sectoral and regional plans, and provides a steer for development cooperation with international partners.⁷¹

The FESR identifies improving mobile phone and Internet services quickly "*to help people access information, create business opportunities, lower transaction costs and enhance social interaction*" as one of its important 'quick wins.' It sets an ambitious target of reaching 80% mobile phone penetration by 2015 and identifies two dimensions of policy reform that are particularly important for a rapid and successful expansion in penetration rates: first, full liberalisation of the market, including opening up to foreign as well as domestic investors; and second, creating an effective regulatory system that ensures competition among suppliers and minimises prices charged to customers.⁷²

The Government's ambitious plans to upgrade its Internet infrastructure is presented as a means to allow a comprehensive e-strategy for leapfrogging in a number of areas: educational programs, Government regulation and knowledge management. The FESR highlights the on-going process of preparing a medium to long term plan for the sector (see below on the different ICT-related Master Plans) and drafting of a *Telecommunications Act* (adopted in 2013 and now in force, see below) that clearly sets out how the Government will separate the policy, regulatory and operational roles of the Government in the sector and establish an independent regulator.⁷³

The FESR focuses on market liberalisation and infrastructure improvements as key drivers of increased mobile penetration and economic development. It recognises the importance of providing digital services such as mobile money, but does not acknowledge the need for security safeguards to protect users and businesses. As the ICT sector has

70 Government of Myanmar, "[Framework for Economic and Social Reform - Policy Priorities for 2012-2015 towards the Long-Term Goals of the National Comprehensive Development Plan \(FESR\)](#)" (January 2013).

71 Tin Maung Maung Than, "[Introductory Overview: Myanmar's Economic Reforms](#)", *Journal of Southeast Asian Economies*, Vol. 31, No. 2 (August 2014).

72 Government of Myanmar, "[Framework for Economic and Social Reform - Policy Priorities for 2012-2015 towards the Long-Term Goals of the National Comprehensive Development Plan \(FESR\)](#)" (January 2013).para. 8.

73 Ibid, para. 78.

developed, stakeholders in the financial services industry have noted that the Central Bank of Myanmar's recent mobile money licenses do not require service providers to adopt specific security standards.⁷⁴

The FESR's operational period is shortly coming to an end in 2015. As such, it is important that the Government's other ICT policy frameworks (see below) reinforce the FESR's commitment to people-centred development by adopting clear and justifiable limits on Government involvement in and access to the ICT sector that are aligned with international standards and best practice (see [Recommendations to the Government of Myanmar](#)).

The 2011-2015 ICT Master Plan

Prior to the FESR (see above), the Government's reform commitments to liberalise the ICT sector in Myanmar were largely contained in three separate ICT Master Plans covering 2001–2005,⁷⁵ 2006–2010,⁷⁶ and 2011–2015. None of the Master Plans were developed or issued by the MCIT or the Government more generally. As a result, many of the objectives lack a clear strategy for robust implementation or enforcement. Instead, the Myanmar Computer Federation (MCF) developed the most recent 2011-2015 ICT Master Plan with support from the Korean International Cooperation Agency and the Electronics and Telecommunications Research Institute (a government supported research institute in Korea). A full version of the Master Plan is not currently available online – only a PowerPoint file providing an overview, rather than the Master Plan itself – meaning specific details as to each of the four functional areas of focus are not publicly available.

The 2011–2015 ICT Master Plan adopts key objectives across four functional areas covering: infrastructure, ICT Industry, ICT Human Resource Development (HRD) and E-education (see Table 6). It sets out various ambitious objectives that are positive from a human rights and social development perspective, including the creation of a research and development centre for ICT security, establishing national software institutes and ICT teacher training programs, and providing Internet access to 1,000 high schools.

The results of the 2011-2015 Master Plan have been mixed, at least in part due to the fact that the Master Plan has not been adopted or enforced as an official Government policy framework. While various objectives such as growing total subscribers (to 30 million by 2015), increasing tele-density (the number of telephone subscriptions per 100 inhabitants) to 50% by 2015⁷⁷ and licensing private operators in the telecommunications sector have been realised, a number of objectives have not yet been achieved. These include (but are not limited to) promoting Myanmar as an ICT outsourcing destination globally, the majority of the stated e-education initiatives and developing a *Cyber Information Act*. In addition, the 2011–2015 ICT Master Plan did not address gaps in the legal framework governing

⁷⁴ See Myanmar Times, "[Preparing the Financial System for Digital Attacks](#)", (March 2015).

⁷⁵ Prepared by the Myanmar Computer Federation (MCF).

⁷⁶ Prepared by the MCF and Republic of Korea under the Initiative for ASEAN Integration.

⁷⁷ MCIT noted that 50% mobile penetration (28.1 million SIM cards) was achieved as of June 2015. See: Myanmar Times, "Mobile Penetration Reaches Half the Country" (June 2015).

ICT operations (specifically concerning intellectual property, freedom of information, lawful interception or data privacy and protection).

Table 6: ICT Master Plan 2011–2015 Action Items across 4 Key ICT Sector Areas

ICT Infrastructure (INF)	ICT Industry (In)	ICT Human Resource Development (HR)	E-education (Ee)
<i>INF1</i> : Demand Path Estimation for ICT Infrastructure Expansion	<i>In1</i> : Develop promotion policies for ICT SMEs and venture businesses	<i>HR1</i> : Develop the ICT network for University	<i>Ee1</i> : Establishment of national committee for information culture movement
<i>INF2</i> : R&D Centre for ICT Security	<i>In2</i> : Give support for the firms in the ICT industry zone	<i>HR2</i> : Set up model schools for ICT (software institutes)	<i>Ee2</i> : Production and distribution of the booklets for promoting information culture
<i>INF3</i> : Tariff Policy	<i>In3</i> : Establish ICT research centre	<i>HR3</i> : Industry University cooperation program for training & R&D collaborations	<i>Ee3</i> : Refresh laws and rules for acceleration of e-Awareness
<i>INF4</i> : Network Migration Roadmap	<i>In4</i> : Enlarge R&D investment and facilities	<i>HR4</i> : Set up a National Research Centre/HRD centre for ICT development	<i>Ee4</i> : Incorporation of ICT training into school curriculum
<i>INF5</i> : Proactive ICT Infrastructure Construction	<i>In5</i> : Increase outsourcing demand of public sector	<i>HR5</i> : Establish and international cooperation network between Myanmar and Foreign ICT University	<i>Ee5</i> : ICT teacher training program
<i>INF6</i> : Promotion of ICT HRD for professional	<i>In6</i> : Develop ICT support tax system	<i>HR6</i> : Set up national certification	<i>Ee6</i> : Development of textbook and contents for ICT training
<i>INF7</i> : Public protection and disaster relief	<i>In7</i> : Expedite market opening and promote international relationship	<i>HR7</i> : Set up digital libraries that connect all other universities	<i>Ee7</i> : Distribution of ICT textbook and contents
<i>INF8</i> : Establishment of a network management centre		<i>HR8</i> : Regional positioning activities as S/W and ICT services outsourcing centre for neighbouring countries	<i>Ee8</i> : Refresh Laws and rules for promotion of digital literacy
<i>INF9</i> : ICT standardisation for the protection of local Industry & expansion of business opportunity		<i>HR9</i> : Incentive policy to foster research personnel	<i>Ee9</i> : National LAN installation and Internet connections for 1000 high schools
<i>INF10</i> : restructure of network service provider (operation and			

Source: MCIT, KOICA, ETRI, “The Follow-Up Project of the Myanmar ICT Master Plan,” (2011)

The Telecommunications Master Plan

On 14 May 2015, MCIT hosted an initial consultation on “*Creating a Master Plan for Myanmar Telecommunications*” in Nay Pyi Taw. The proposed Master Plan outline covered rural and regional development, roles and responsibilities of MCIT, PTD, other Government bodies and MPT and other operators, as well as key topics forming a ‘reference framework’, including Net Neutrality (the principle of treating Internet traffic and content delivery in a neutral manner, without throttling or preferentially accelerating access), universal service, and privacy and security.

Table 7: Proposed Vision of the 2015 Draft Telecommunications Master Plan, as of August 2015

The draft Master Plan sets out three broad goals:

- to create a Myanmar national broadband infrastructure with affordable services
- to deliver communications content and services for the Myanmar people in a rights-respecting, mobile-first system
- to develop an institutional and policy framework for effective oversight

Source: [Draft Telecommunications Master Plan 2015](#)

In late July 2015, a draft Telecommunications Master Plan was published for public consultation through 7 August 2015 (Table 7).⁷⁸ Several organisations, including the Myanmar Centre for Responsible Business (MCRB), MIDO and Access (a US based digital rights organisation), provided comments on the draft Masterplan.⁷⁹ Both MCRB and Access called for:

- A commitment not to shut down communications networks, as the Myanmar Government did in 2007 (See [Chapter 4.1](#) on Freedom of Expression)
- The release of ‘transparency reports’ by Myanmar’s regulatory bodies to provide the public with information about Government access to user data (See 4.4 on Surveillance) and by telecommunication companies (noting that Telenor has already done this)
- A data protection system that informs and protects users, while also encouraging innovation (See [Chapter 4.5](#) on Cybersecurity)
- A lawful intercept framework including access to remedy (see the [Annex to the Recommendations](#))
- A commitment to Net Neutrality, which is fundamental to ensure that the Internet remains a platform for the enjoyment of human rights and innovation

⁷⁸ Myanmar Ministry of Communications and Information Technology, “[Draft Telecommunications Masterplan](#)” (8 July 2015).

⁷⁹ MCRB, “[Comments on the draft Myanmar Telecommunications Master Plan](#)” (30 July 2015).

When delivering services to the Myanmar people, MCRB recommended that services should be widely available in Burmese and also in ethnic languages in the ethnic regions. In addition, MCRB highlighted that time should be given to ensure local level stakeholder engagement and communication with regards to building towers and laying fibre, and requiring and enforcing adequate health and safety protection for workers involved (See [Chapter 4.6](#) on Labour and [Chapter 4.7](#) on Land).

The E-Governance Master Plan

Myanmar is currently developing an E-Governance Master Plan 2015 with support from the Asian Development Bank (ADB)⁸⁰. The Government is focusing on streamlining its processes to improve efficiency through the development of a common framework for ICTs, transparency and a wider reach of public service delivery. The Master Plan will guide continuous and more detailed planning in the areas covered. For example, the Master Plan lays out a conceptual architecture for cybersecurity, while the detailed operationalisation will be developed to meet the needs and specific characteristics of evolving e-governance interventions.

A draft E-Governance Master Plan shared with the ICT Sector Working Group focuses on the use of ICTs in the reform of public-sector processes to implement a coherent and systematic approach to the design, evaluation and adoption of the systems underpinning public services to improve their delivery and efficiency. Out of a total of 21 Government Ministries, only nine are included in the draft Master Plan.⁸¹ Process reform is intended to be supported by common infrastructure and shared software applications among the nine participating Ministries.

The common shared software being used across these ministries is intended to focus on areas that will improve operational efficiency and communication within the Government, including email, human resources management and payroll, and e-office tools. Under the E-Governance Master Plan, the MCIT is also tasked with developing a 'citizen service centre'. It is unclear if this task overlaps with the Myanmar National Portal (to provide accessible public information on Government services) being developed under the World Bank's Telecommunications Sector Reform Project (see section A above)⁸² and what

80 ADB, "Project 47158-001: Design of e-Governance Master Plan and Review of Information and Communication Technology Capacity in Academic Institutions" (2013)

81 Participating ministries include the: Ministry of Communications and Information Technology, Ministry of Construction, Ministry of Power, Ministry of NPED, Ministry of Commerce, Ministry of Transport, Ministry of Home Affairs, Ministry of Rail Transport. It is unclear why these ministries, and not others (or all), are participating.

82 The World Bank's Telecommunications Sector Reform project calls for the development of "A mobile friendly Myanmar National Portal (\$ 3.62 million) will be financed to provide citizens, businesses, and visitors (comprising of foreign workers, investors and tourists) with a single window into the information and services offered by the Government. Over time the National Portal will allow its users to find relevant information, provide suggestions and feedback, and transact services in a safe and convenient electronic environment."

services would be offered through the citizen service centre beyond e-payments from citizens to Government.⁸³

It is currently unclear how protection of the right to privacy will be incorporated into the Master Plan's design, any implementation of e-Governance practices within Government apparatus, or any future e-Government related regulations. User trust is central to the concept of ICTs and e-Governance. If people and businesses do not believe that their personal data will be safe and secure from unwarranted surveillance or misuse, then they will be less likely to use e-Government and other services. This could undermine the Master Plan's ability to support accountability, transparency and progress in human rights and social development in Myanmar.⁸⁴ (See further [Chapter 4.3](#) on Privacy and the [Recommendations to the Myanmar Government](#)).

Regional Policy Frameworks: The 2015 ASEAN ICT Master Plan

The 2015 ASEAN ICT Masterplan was developed by Government Ministers, policy makers, regulators and the ICT industry within the ASEAN region. It focuses on three pillars – economic transformation, people empowerment and engagement – supported by a foundation of infrastructure development, bridging the digital divide and human capital development.⁸⁵ Recognising the key transformational role that ICT can play in promoting economic development and integration, it is also acknowledges and encourages the role of ICT in building more empowered and inclusive societies “*involving all the stakeholders in ASEAN – government, citizens and businesses, developed and developing, rural and urban, young and old, as well as those with and without disabilities*”. The Master Plan is to be implemented over the next five years.

While stakeholder consultations highlighted the need for more transparency,⁸⁶ the Master Plan does not address the role of ICT in improving transparency and accountability, nor does it address the sector's important role in promoting freedom of speech. The Master Plan will therefore will provide little guidance to the Government of Myanmar in finding the appropriate balance in improving accountability, transparency and the protection of human rights in developing its regulatory framework.

⁸³ See: ADB, “[Myanmar: Design of e-Governance Master Plan and Review of Information and Communication Technology Capacity in Academic Institutions](#)” (last accessed August 2015).

⁸⁴ US Campaign for Burma et al, “[Civil Society Comments on the World Bank Telecom Sector Reform Project in Burma](#)” (21 January 2014), p. 3.

⁸⁵ ASEAN, “ASEAN ICT Masterplan 2015” (2011).

⁸⁶ *Ibid*, pg. 10.

C. International Legal Framework Relevant to Myanmar's ICT Sector

Until very recently, Myanmar had acceded to relatively few international human rights treaties.

Table 8: Myanmar's Accession to International Human Rights Instruments

Myanmar has acceded to:

- International Covenant on Economic, Social and Cultural Rights (ICESCR) (signed July 2015)
- Convention on the Elimination of Discrimination Against Women (CEDAW)
- Convention on the Rights of Persons with Disabilities (CRPD)
- Convention on the Rights of the Child (CRC) & the Optional Protocol on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography
- Three of the eight ILO Fundamental Conventions:
 - Forced Labour Convention (ILO Convention 29)
 - Freedom of Association and Protection of the Right to Organise Convention (ILO Convention 87)
- Worst Forms of Child Labour Convention, No 182 (entered into force December 2014)
- Nineteen of the 177 Technical Conventions of the ILO, including the ILO Hours of Work (Industry) Convention
- Convention against Transnational Organised Crime, and its supplementary Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children and Protocol against the Smuggling of Migrants by Land, Sea and Air
- UN Convention against Corruption
- Geneva Conventions I-IV
- Convention on the Prevention and Punishment of the Crime of Genocide
- UN Convention for the Safeguarding of the Intangible Cultural Heritage

Myanmar has not signed:

- International Covenant on Civil and Political Rights (ICCPR)
- International Convention on the Elimination of All Forms of Racial Discrimination (CERD)
- Convention Against Torture and Other Cruel, Inhuman and Degrading Treatment (CAT)
- Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW)
- International Convention for the Protection of All Persons from Enforced Disappearance (CED)
- Optional Protocol to the Convention on the Elimination of Discrimination against Women (OP-CEDAW)
- Optional Protocol to the Convention on the Rights of the Child on the

involvement of children in armed conflicts (OP-CRC-AC)

- Optional Protocol to the Convention on the Rights of Persons with Disabilities (CRPD-OP)
- Five of the eight ILO Fundamental Conventions:⁸⁷
 - Right to Organise and Collective Bargaining Convention No. 98
 - Equal Remuneration Convention No. 100
 - Abolition of Forced Labour Convention No. 105
 - Discrimination (Employment and Occupation) Convention No. 111
 - Minimum Age Convention, 1973 (No. 138)
- 158 out of the 177 ILO Technical Conventions
- Any of the four ILO Governance Conventions

In addition, the Government reportedly has not conducted any assessment of the compatibility of its existing laws with its obligations under international law.⁸⁸ Domestic courts cannot directly invoke the provisions of international or regional human rights instruments to interpret national laws unless such standards are incorporated into national legislation.⁸⁹ While it is not unusual for international law not to be automatically incorporated into domestic law, one implication of this is that Myanmar's judiciary cannot have recourse to international human rights law to circumscribe the wide discretionary powers that Myanmar's laws confer on the executive branch.

D. Domestic Legal Framework Governing Myanmar's ICT Sector

This section analyses the ICT-specific Myanmar laws in Table 9, and how the interpretation of their provisions could result in negative impacts on human rights. It should not, however, be taken as a description of how these provisions have been used in practice. That said, many of the pre-2011 laws have been used to jail political activists and human rights defenders.

It explains how even provisions identified in more recent laws might perversely require ICT companies to assist the Government to arbitrarily restrict certain rights, in order to maintain their legal licenses. Table 21 at the end of this Chapter also identifies key provisions of concern from other domestic laws not specific to ICTs that could be, and in some cases have been, used to infringe the rights to freedom of expression or association.

⁸⁷ ILO Normlex, "[Up-to-date Conventions not ratified by Myanmar](#)" (last accessed August 2015).

⁸⁸ DLA Piper et al, [Myanmar Rule of Law Assessment](#) (March 2013), p. 27.

⁸⁹ UN General Assembly, "[Compilation prepared by the Office of the High Commissioner for Human Rights in accordance with paragraph 15 \(b\) of the annex to Human Rights Council resolution 5/1, Myanmar](#)", A/HRC/WG.6/10/MMR/2 (15 Nov 2010), para. 5.

Table 9: Principal Existing Domestic Laws Relevant to ICTs

<p>ICT-specific Domestic Laws:</p> <ul style="list-style-type: none"> ■ Telecommunications Law (2013) ■ Electronic Transactions Law (2004) ■ Computer Science Development Law (1996) <p>Laws Related to Freedom of Association Relevant to the Use of ICTs:</p> <ul style="list-style-type: none"> ■ Law Relating to the Registration of Organisations (2014) ■ Unlawful Associations Act (1908) <p>Other Domestic Laws at Risk of Infringing Human Rights Relevant to the Use of ICTs:</p> <ul style="list-style-type: none"> ■ Emergency Provisions Act (1950) ■ Official Secrets Act (1923) ■ Myanmar Constitution (2008) ■ Penal Code of Burma (1957)

Table 10: Existing Gaps in Myanmar's ICT Legal Framework

<p>There are a number of substantive areas currently unaddressed under Myanmar laws or regulations. These represent major gaps in the protection of Myanmar people, ICT users and ICT companies. They include:</p> <ul style="list-style-type: none"> ■ Data Privacy ■ Data Protection ■ Access to Information ■ Cybercrime ■ Lawful Interception ■ Intellectual Property

Table 11: Summary of Human Rights at Risk under Domestic ICT Laws

	Freedom of Expression	Right to Privacy	Equality of Access
Telecommunications Law (2013)	<ul style="list-style-type: none"> – Criminalisation of legitimate expression: s68(a) & (b) and s66(c) & (d) – Arbitrary blocking or filtering of content: s77 – Arbitrary disruption or disconnection of Internet access: s77 	<ul style="list-style-type: none"> – Government monitoring and surveillance of user activity and content: s77 & s78 – Government access to user-identifying data and the right to anonymity: s75 & s77 	<ul style="list-style-type: none"> – Equality of Access to information and benefits of ICTs for the rural poor, and ethnic, cultural and religious minorities: s55

<p>Electronic Transactions Act (2004)</p>	<ul style="list-style-type: none"> - 7-15y imprisonment and/or fines for using technology to do acts detrimental to “state security” or “community peace and tranquillity” and other vague and undefined terms: s33(1) & (b) - 5y imprisonment and/or fines for creating, modifying or distributing information detrimental “to the interest of or to lower the dignity of any organisation or any person”: s34(d) 	<ul style="list-style-type: none"> - Broad powers granted to a “Control Board” able to access and inspect any ICT it has “reasonable cause” to suspect was involved in an offence under the Act: Ch. V.9 	
<p>Computer Science Development Law (1996)</p>	<ul style="list-style-type: none"> - 7-15y imprisonment for anyone using a computer or network to engage in “any act” which undermines e.g. “state security” or “community peace and tranquillity” and other vague and undefined terms: s35 		

2013 Telecommunications Law

Background, Scope and Objectives

The recent *Telecommunications Law* (No. 31/2013) was adopted in October 2013, revoking the 1885 *Myanmar Telegraph Act* and 1934 *Myanmar Wireless Telegraphy Act*.⁹⁰ It also reportedly replaces the Wide Area Network Order (No. 3/2002).

Objectives of the 2013 *Telecommunications Law* include:⁹¹

- Supporting the modernisation and development of the nation with telecommunications technology
- Enabling telecommunications services that will be able to provide high quality and worthy (sic) services to users by allowing fair and transparent competition from domestic and abroad in the telecommunications sector which is developing
- Giving more opportunities to the general public to use the telecommunications service by expanding the telecommunications network in the entire country along with the telecommunications technology which is developing
- Protecting telecommunications service providers and users in accord with the law, including through consumer protection standards

90 See [DFDL unofficial translation of Myanmar Telecommunications Law](#) (No. 31/2013).

91 See Section 4, *Myanmar Telecommunications Law* (No. 31/2013)

- Supervising telecommunications service, network facilities and telecommunications equipment which require license for national peace and tranquility and for public security

The 2013 *Telecommunications Law* outlines the duties and rights of both telecommunications service providers and regulators, and sets out at high level the licensing regime for the provision of certain telecommunications services, including:

- the provision or operation of infrastructure or network facilities
- the provision of service for transmission and reception of information
- the provision of services by way of transmitting and receiving

See Table 25 in [Chapter 3](#) for the specific types of licenses that have subsequently been issued.

Risks to the Right to Freedom of Expression

Risks related to the violation of freedom of opinion and expression under the 2013 *Telecommunications Law* can be categorised into at least three areas of concern:

- criminalisation of legitimate online expression;
- arbitrary blocking or filtering of content, and;
- arbitrary disruption and disconnection of Internet access.

These are considered in more detail below.

Criminalisation of legitimate expression online

The 2013 *Telecommunications Law* maintains some of the troubling provisions of the laws it replaces. Punishable offenses include using a telecommunications network to “*to extort, threaten, obstruct, defame, disturb, inappropriately influence or intimidate*”. These are vague terms that are not defined in the Law. This creates a clear risk that the Myanmar Government could use the 2013 *Telecommunications Law* to arbitrarily characterise legitimate expression as “*threats*” or an “*inappropriate influence*”, punishable as a criminal offense (see Table 12 below).

Table 12: Provisions of the 2013 Telecommunications Law with Potential to be used to Criminalise Legitimate Expression

- Content-related offenses punishable by up to 3 years’ imprisonment and/or fines include “*using a telecommunications network to steal money and property, cheat and embezzle or harming the interests*” [sic] (s66(c)), or “*to extort, threaten, obstruct, defame, disturb, inappropriately influence or intimidate.*” (s66(d))
- Content-related offenses punishable by up to one years’ imprisonment and/or fines include “*connecting, receiving, transmitting, distributing or handing out false information dishonestly*” (s68(a)) or “*unauthorised prohibition, forbidding obstruction to the transmitting, receiving, communication, handing out or distribution of information.*” [sic] (s68(b))

In addition to the risk that an end user's exercise of legitimate expression or opinion will be criminalised, ICT companies – telecommunications companies, network service providers, online publishing platforms, amongst others – may also be at risk of facilitating the allegedly criminal conduct by its users on their networks or platforms. Government-issued telecommunications service licenses are required for any entity to become a service provider (s5). Licensees are subject to suspension or termination of licenses for failure to comply with a broad set of conditions, which can include requests from Government concerning the blockage or restriction of content deemed criminal (s57). This could create a perverse incentive for ICT companies to contribute to the arbitrary criminalisation of legitimate expression in order to maintain their legal license to operate. In particular:

- The definition of “*network service provider*” includes any “*service for carrying information two ways by any means of tele-communication*” [s3(h)], meaning ICT companies are subject to these licensing risks.
- Even if the companies are not explicitly mentioned in relevant laws, language referring to the “*distribution*” or “*dissemination*” of prohibited speech could be construed as “*abetting*” the allegedly criminal behaviour, and subject to the same punishment (s73).
- The provision prohibiting “*connecting, receiving, transmitting, distributing or handing out false information dishonestly*” may also implicate ICT companies transmitting content (s68(a)).
- In general, the above provisions could also be used to compel ICT company to comply with Government requests to arbitrarily block or filter user content (see below).

Arbitrary blocking or filtering of content

The 2013 *Telecommunications Law* also provides legal capacity for the Myanmar Government to potentially block or filter user content selectively and arbitrarily (see Table 13). The law enables the Government, without clear oversight, to “*prohibit a specific type of communication,*” if doing so is “*in the interest of the public*” – a very broadly worded and vague standard.

Table 13: Provisions of the 2013 Telecommunications Law with Potential to be used to Arbitrarily Block or Filter User Content

- The Government may, “*when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee to suspend the telecommunications service provider business, prohibit a specific type of communication, to block and hold [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment.*” (s77)

As above, because licensees are subject to suspension or termination of licenses (s5) for failure to comply with a broad set of conditions (s57), there may be strong incentive for ICT companies to take action to block or filter content to avoid revocation of their license, creating a risk of contributing to Government actions in violation of freedom of expression and opinion. In particular:

- Licensees must “*make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law.*” (s78) While this section appears to primarily justify network disconnection/suspension, it could be used to block whole websites.
- In general, the provisions cited above regarding ICT company facilitation of allegedly criminal expression may also be used to compel the ICT company to arbitrarily block or filter user content in order to avoid revocation of their license.

Arbitrary Disruption or Disconnection of Internet Access

In a world in which services such as government, health and education, are increasingly on-line and digitised, users’ exercise of a wide range of human rights is tied to access to ICTs. In the case of a total network shutdown, these rights may be denied altogether.

Furthermore, in the context of a violent crackdown or other crisis, failure to broadcast news and images domestically and internationally could exacerbate violations of civil and political rights by allowing them to take place behind closed doors. During the violent crackdown against protestors in 2007 (the ‘Saffron Revolution’), the Myanmar Government suspended Internet services, among other actions.

The 2013 Telecommunications Law allows for the Government to suspend or take control of telecommunications services (Table 14), but the situations in which the Government can exercise this power are unclear under the Law. The Government has not made any public commitments regarding network shutdowns during the forthcoming November 2015 elections.

Table 14: Provisions of the 2013 Telecommunications Law with Potential to be used to Arbitrarily Disrupt or Disconnect Internet Access

- Explicitly allows the Government to “*when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee to suspend the telecommunications service provider business, prohibit a specific type of communication, to block and hold [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment*” (s77).

Again, the *2013 Telecommunications Law* puts ICT service companies at risk of contributing to Government measures to arbitrarily disrupt or disconnect Internet access, due to the threat of their legal licence to operate (s5) being revoked for failure to comply (s57). In particular:

- In order to comply with s77 (Table 14), “[t]he licensee shall ... *make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law.*” (s78)

Risks to the Right to Privacy

Section 69 of the 2013 *Telecommunications Law* requires a court order for the disclosure of information kept in secured or encrypted systems. However the Myanmar Government has yet to draft implementing regulations governing the interception of communications by law enforcement authorities.

The Government has expansive powers under the 2013 *Telecommunications Law* to, for example, “*enter and inspect*” telecommunication services when “*in the public interest*” or “*intercept*” communications when an “*emergency situation*” arises. Implementing regulations are therefore necessary to provide clarity on the appropriate restrictions and procedures for the exercise of that power. The [Annex to the Recommendations](#) of this SWIA provides guidance on a rights-respecting framework for lawful interception that sets out the kind of restrictions on that power of interception that the Government should take into account in drafting its framework.

Risks related to the violation of the right to privacy under *the 2013 Telecommunications Law* cover two closely related areas of concern:

- Government monitoring and surveillance of user activity and content, and;
- Government access to user-identifying information and the implications for emerging international norms around the right to anonymity.

Government monitoring and surveillance of user activity and content

The Myanmar Government has a long history of close surveillance of its people. Despite ongoing reforms, the 2013 *Telecommunications Law* maintains a legal basis for monitoring communications and content. While the justification for surveillance is “*security matters*”, the risk of arbitrary and / or overly broad interpretation of that provision is high (see Table 15 below).

Table 15: Provisions of the 2013 Telecommunications Law with Potential to be used to Monitor User Activity and Content

- The Government may, “*when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee ... to retrieve necessary information and communications [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment.*” (s77)

Risks of Company Involvement in Human Rights Violations

Implementing regulations of the 2013 *Telecommunications Law*, once available, may provide more guidance on the scope of expected ICT company cooperation with Government-ordered surveillance of ICT users. Currently, the *Telecommunications Law* as written leaves ICT companies open to significant risk of involvement in Government surveillance activities in a way which does not meet international standards of human rights protection.

Again, since Government-issued telecommunications service licenses are required for any entity to become a service provider (s5), licensees are subject to suspension or termination of licenses for failure to comply with a broad set of conditions (s57). This can include surveillance, and could therefore create perverse incentives for ICT companies to contribute to the arbitrary monitoring and surveillance of user activity by the Myanmar Government in order to maintain their legal license to operate. In particular:

- Government authorities, “for defense and security matters of the State or for the public interest, if necessary ... may enter into the premises of the licensed telecommunication services provider and inspect, supervise and request the licensee to submit records regarding the services.” (s76)
- The *Telecommunications Law* also provides explicit Government authorisation “to retrieve necessary information and communications [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment.” (s77)
- Accordingly, licensees must “make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law.” (s78)

Government access to user-identifying information and implications for the right to anonymity

There is a growing international concern among human rights observers about government policies throughout the world which can compromise the ability of individuals to express themselves anonymously on the Internet. The provisions of the 2013 *Telecommunications Law* could be used to override anonymity, and may constitute a separate basis for violation of the right to privacy (Table 16). This may risk further undermining confidence and security on the Internet, impeding the free flow of information and ideas online.

Table 16: Provisions of the 2013 Telecommunications Law with Potential to be used to Grant Government Access to User-Identifying Information

- In order “[t]o obtain any information or communications that may adversely affect the security of the State, the rule of law and order, the Union Government may direct the relevant organisations as necessary without infringing upon the original rights of the citizens.” (s75)
- The Government may also, “when the situation arises to carry out in the interest of the public, with the approval of the government, direct the licensee to... to retrieve necessary information and communications [and] to temporarily control and use the telecommunications service provider businesses and telecommunications equipment.” (s77)

Risks of Company Involvement in Human Rights Violations

Where ICT companies comply with unreasonable, overbroad, or otherwise questionable Government requests for user data under Myanmar law, they may be involved in

threatening anonymous expression and privacy online. As above, since Government-issued telecommunications service licenses are required for any entity to become a service provider (s5), licensees are subject to suspension or termination of licenses for failure to comply with Government requests to access user-identifying information (s57). In particular:

- Licensees must “*make necessary preparations to enable a telecommunication service to be utilised for security matters in accordance with the law.*” (s78)
- Moreover, Government authorities, “*for defense and security matters of the State or for the public interest, if necessary ... may enter into the premises of the licensed telecommunication services provider and inspect, supervise and request the licensee to submit records regarding the services.*” (s76)

Positive Aspects on Promoting Equality of Access to ICTs

Under the 2013 *Telecommunications Law* Myanmar Ministries may create programmes for extending services to underserved areas of the country. The Myanmar Government has shown readiness in practice to achieve equality of access to ICTs (see further [Chapter 3](#) on Sector-Level Impacts). For example:

- President Thein Sein publicly noted the importance of strengthening telecommunications access in rural areas.⁹² In response, Ministry officials announced a plan to allow purchase of SIM cards in installments, with the stated aim of encouraging access for rural citizens⁹³. (The need for this was subsequently overtaken by the introduction of competition in the market which led SIM Card prices to fall from 150,000 MMK to 1,500 MMK).
- In March 2015 Myanmar joined the Alliance for Affordable Internet (AFAI).⁹⁴ AFAI’s goal is to realise the “*UN Broadband Commission’s target of entry-level broadband priced at less than 5% of monthly income*”.⁹⁵
- In addition, each telecommunications Operator Licence includes the requirement that after three years (assuming network rollout targets are met), the operator must contribute 2% of annual revenue to a Universal Service Fund managed by MCIT that is intended to subsidise the cost of telecommunications service in areas where infrastructure deployment is not economically viable for network operators.

⁹² See: The Republic of the Union of Myanmar President’s Office, “[Speeces and Remarks](#)” (last accessed August 2015).

⁹³ Myanmar Times, “[SIMs for sale by instalment in rural areas, says MPT](#)” (8 October 2012).

⁹⁴ An ICT sector coalition that focuses on combining advocacy, research, and knowledge sharing to influence broadband policy.

⁹⁵ Alliance for Affordable Internet, “[Vision and Strategy](#)” (last accessed August 2015).

Electronic Transactions Law (2004)

Background, Scope and Objectives

With support from the Myanmar Computer Federation (MCF) and technical assistance from the World Bank, MCIT is in the process of reviewing the 2004 *Electronic Transactions Law*.⁹⁶ A draft of the revised law is not publicly available and there are no indications as to whether there will be public consultation on any future draft.

The 2004 *Electronic Transactions Law* as currently drafted focuses on the authenticity of electronic data as well as electronic contracts. The law also establishes a Control Board and licensing process for certification authorities in Myanmar able to issue digital certificates used to authenticate electronic communications. When information is exchanged securely online, digital certificates provide information that is used to verify the sender and recipient's identity. Under s34(a) the law criminalises hacking and unauthorised interception of communications.⁹⁷

A draft “*Cyber-Security Law*” is also reportedly in preparation, although it is unclear if the Ministry of Home Affairs or MCIT will support MCF in drafting. (See further [Chapter 4.5](#))

Risks to the Right to Freedom of Expression and Privacy

Though reportedly on the verge of revision, the 2004 *Electronic Transactions Law* has been used to restrict online speech deemed to be “*detrimental to the security of the state*” or “*community peace and tranquillity*”, amongst other vague and undefined terms (Table 17). Between 2007 and 2009 several journalists and online activists were sentenced to long prison terms under this law, though have all since been released and it has not been used since 2011.⁹⁸

Table 17: Provisions of the Electronic Transaction Law with Potential to be used to Infringe Freedom of Expression and Privacy

- Anyone “*using electronic transactions technology*” to do “*any act detrimental to the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture,*” or engage in “*receiving or sending and distributing any information relating to secrets of the security of the State or prevalence of law and order or community peace and tranquillity or national solidarity or national economy or national culture,*” may be imprisoned for 7-15 years and/or fined. (s33(a)-(b))
- Anyone found “*creating, modifying or altering of information or distributing of*

⁹⁶ [Myanmar Electronic Transactions Law](#) (2004). In January 2013, lawmaker Thein Nyunt from the New National Democracy Party proposed a bill that would abolish the law, but it was rejected by the lower house. Instead he decided to amend it, and a bill to amend the law was submitted August 21, 2013 for consideration. A committee to create the new draft includes parliamentarians, NGOs, industry organizations, and others. See Radio Free Asia, “[Myanmar’s Parliament Considers Amending Draconian Law](#)” (21 August 2013).

⁹⁷ See [The Electronic Transactions Law](#) (No. 5/2004), Art. 34(a).

⁹⁸ Specifically, Hla Hla Win, Myint Naing, Ngwe Soe (Tun Kyaw), Nay Phone Latt, Maung Thura (Zarganar), Kaung Myat Hlaing (Nat Soe), Win Maw, and Zaw Thet Htwe were imprisoned under the Electronic Transactions Act, and were all released between 2011 and 2012.

information created, modified or altered by electronic technology to be detrimental to the interest of or to lower the dignity of any organisation or any person” may be imprisoned for 5 years and/or fined. (s34(d))

- Chapter V Formation of the Electronic Transactions Control Board and Functions and Powers thereof

9. The Central Body:

(i) having access to and inspecting and checking the operation of any computer system and any associated apparatus or material which it has reasonable cause to suspect is or has been in use in connection with any offence under this Law;

(j) exposing and acquiring any necessary identification document from any person with respect to any offence contained in this Law;

Risks of Company Involvement in Human Rights Violations

ICT companies could be implicated in assisting alleged criminal offences under the *Electronic Transactions Law*. As with the 2013 *Telecommunications Act* (see above), there are provisions that tie the revocation or suspension of ICT companies’ licences to compliance with Government conditions, which has the potential to cause adverse impacts to users’ rights to freedom of expression and/or their privacy. These provisions include:

- The law states that “[w]hoever attempts to commit any offence of this Law or conspires amounting to an offence or abets the commission of an offence shall be punished with the punishment provided for such offence in this Law.” (s38)
- 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. (s28).

Computer Science Development Law (1996)

Background, Scope and Objectives

The Ministry of Science and Technology is in the process of revising the 1996 *Computer Science Development Law* which was intended to accelerate the growth of technology in Myanmar⁹⁹. The new law is to be named the “*Information Technology Development Law*” and is being drafted with support from the Myanmar Computer Federation (MCF). A draft of the revised law has reportedly been sent to the President’s Office before a public review.

⁹⁹ [Myanmar Computer Science Development Law](#) (1996).

Risks to Right to Freedom of Expression

Similar to the 2004 *Electronic Transactions Law*, the 1996 *Computer Science Development Law* provides for lengthy terms of imprisonment for anyone using a computer to do anything that undermines “*community peace and tranquillity*”, “*national unity*” and other vague and undefined conduct (Table 18). It also puts limitations on use of ICTs. Criminal penalty could result from connecting to or establishing a “*computer network*” without MCIT permission.

Table 18: Provisions of the Computer Science Development Law with Potential to be used to Infringe Freedom of Expression

- Anyone “*using computer network or any information technology*” to engage in “*carrying out any act which undermines State Security, prevalence of law and order and community peace and tranquillity, national unity, State economy or national culture*” or “*obtaining or sending and distributing any information of State secret relevant to State security, prevalence of law and order and community peace and tranquillity, national unity, State economy or national culture*” may be imprisoned for 7-15 years and/or fined. (s35)
- Anyone wishing to establish “*a computer network or connecting a link inside the computer network*” must apply for prior permission from the MCIT. (s29)

Risks of Company Involvement in Human Rights Violations

ICT companies could be liable for abetting offences under the *Computer Science Development Law*. In particular:

- “*Whoever attempts or conspires to commit any offence under this law or abets in the commission of such offence shall, on conviction be punished with the same penalty prescribed in this Law for such offence.*” (s38)

This again raises the risk that if ICT companies, in order to maintain their legal licenses to operate, comply with Government measures to restrict computer use, they may as a result be involved in adverse human rights impacts caused by the Myanmar Government.

Law Relating to the Registration of Organisations (2014)

Background, Scope and Objectives

For decades the Myanmar authorities greatly restricted the right to form organisations and arrested those attempting to do so. In 1988 the military government issued a Decree called the *Associational Law* (Law No. 6/88), which named categories of banned organisations and provided for harsh terms of imprisonment and fines for people belonging to these organisations. However as part of the political, economic and legal reform process, which began in 2011, new efforts were made to change laws governing freedom of association. The culmination of such work by CSOs and Parliament was the enactment of the *Law relating to Registration of Organisations* in July 2014. The law

annulled *Law No 6/88* (Article 43), thereby increasing the political space for CSOs and others to form organisations.

Risks to Right to Freedom of Association

An early draft of the *2014 Law Relating to Registration of Organisations* required all groups to be formally registered, with severe penalties for failing to do so. The law was adopted in July 2014 with this provision removed. However it retains another provision of concern to CSOs, which requires groups who do decide to register to do so at township, state or national level. This thereby potentially restricts their area of operation, since organisations that register in one township would only be able to operate in that township.¹⁰⁰ The website of the International Centre for Not-for-Profit Law (ICNL) provides further information on laws relating to Myanmar civil society.¹⁰¹

Table 19: Provisions of the Law Relating to the Registration of Organisations with Potential to be used to Infringe the Right to Freedom of Association

- Prohibited organisations include those “*that attempt, instigate, incite, abet or commit acts that may in any way disrupt law and order, peace and tranquility, or safe and secure communications*” and “*Organisations that attempt, instigate, incite, abet or commit acts that may [affect] or disrupt the regularity of state machinery*” (s5)
- “*Any person found guilty of committing an offence...shall be punished with imprisonment for a term which may extend to five years.*” (s6)

Risks of Company Involvement in Human Rights Violations

Read broadly, ICT companies found to be providing services to such prohibited organisations might be accused of ‘abetting’ them. In particular:

- Anyone found “*aiding and abetting...organisations that are not permitted to form or not permitted to continue in existence...shall be punished with imprisonment for a term which may extend to three years.*” (s7)

An ICT company, to avoid liability or revocation of their license, might therefore take steps to contribute to a restriction of an organisation’s right to freedom of association (or expression).

Unlawful Associations Act (1908)

Background, Scope and Objectives

A number of laws restricting freedom of expression and association in Myanmar are still in force, in spite of the legal reform process which began during 2011. Among them is the colonial era *1908 Unlawful Associations Act*.

¹⁰⁰ DVB, “[Activists relay worries of draft association law to parliament](#)” (5 June 2014).

¹⁰¹ ICNL, “[NGO Law Monitor: Myanmar \(Burma\)](#)” (last accessed August 2015).

Risks to the Right to Freedom of Association

The 1908 *Unlawful Associations Act* has often been used in the past to imprison peaceful critics of the Government. Article 15 (2) (b) defines an organisation to be unlawful “*which has been declared unlawful by the President...*” i.e. based solely on the head of state’s opinion rather than on reason or evidence. Under Article 17 (1), not only can a member of an illegal organisation be imprisoned, but anyone in any way associated with an unlawful organisation is also at risk of imprisonment. Article 17 (2) provides for imprisonment of leaders of illegal organisations. Article 15 (2) (a) also defines illegal organisations as those involved in violence, often ethnic minority armed opposition groups.

While states need to protect its citizens from violence,¹⁰² there is concern that this provision has been used against ethnic minority civilians not involved in violence. Although the *Unlawful Associations Act* is now less frequently used, ethnic minority civilians in armed conflict areas have recently been sentenced under its provisions.¹⁰³ It remains of concern to anyone involved in the peace process since non-state armed groups are considered ‘unlawful associations’ even though they are negotiating a nationwide ceasefire with government.

Table 20: Provisions of the Unlawful Associations Act with Potential to be used to Infringe the Right to Freedom of Association

- Under the law, “*unlawful association means an association which encourages or aids person to commit acts of violence or intimidation or of which the members habitually commit such acts, or which has been declared to be unlawful by the President.*” (s15(2))
- In addition, “*Whoever is a member of an unlawful association, or takes part in meetings of any such association, or contributes or receives or solicits any contribution for the purpose of any such association or in any way assists the operations of any such association, shall be punished with imprisonment for a term [which shall not be less than two years and more than three years and shall also be liable to fine].*” (s17)

Risks of Company Involvement in Human Rights Violations

Read broadly, an ICT utilised for the purpose of organising a meeting, or broadcasting the communications, of an “*unlawful association*” could be held liable since:

- Anyone who “*assists in the management of an unlawful association, or promotes or assists in promoting a meeting of any such association, or of any members thereof as such members, shall be punished with imprisonment for a term [which shall not be less than three years and more than five years and shall also be liable to fine].*” (s17(2))

¹⁰² Amnesty International, “[Myanmar: Justice on Trial](#)”, (July 2003), pg 28 – 33.

¹⁰³ See for example Fortify Rights, “[‘I thought they would kill me’, Ending Wartime Torture in Northern Myanmar](#)” (June 2014), pg 40-41 and 42-43.

Table 21: Provisions of other Domestic Laws at Risk of Infringing the Rights to Freedom of Expression and Freedom of Association and Raising Potential Liability

Freedom of Expression
<p>Penal Code (1957) ¹⁰⁴</p> <p>Key Provisions of Concern:</p> <ul style="list-style-type: none"> – s121: Authorises death penalty for anyone who “<i>incites</i>” the “<i>commission of treason</i>”. – s123 & s124: Authorises imprisonment for anyone who “<i>encourages</i>” the commission of treason or “<i>by words... attempts to bring into hatred or contempt, or excites dissatisfaction (or attempts) towards</i>” the Government. – Although these provisions do not explicitly specify electronic communications, this could be implied from the provisions. <p>Provisions raising potential liability for ICTs:</p> <ul style="list-style-type: none"> – s124B: Anyone who “<i>knowingly or willfully prints, publishes, edits, issues, circulates, sells, distributes, or publicly displays any written or printed matter which advocates, advises, or teaches the duty, necessity, desirability or propriety of overthrowing or destroying any such organ by force or violence...shall be punished with imprisonment of either description for a term which may extend to not less than three years and not more than ten years, and shall also be liable to fine.</i>”
<p>Emergency Provisions Act (1950) ¹⁰⁵</p> <p>Key Provisions of Concern:</p> <ul style="list-style-type: none"> – s5: Up to 7 years imprisonment for communication that “<i>alarm[s]</i>” people in a way that would create panic, or “<i>spread[ing] false news, knowing, or having reason to believe that it is not true,</i>” and “<i>affect[ing] the morality or conduct of the public/a group...in a way that would undermine the security of the Union or the restoration of law and order</i>”. – Although this provision does not explicitly specify electronic communications, such expression could be covered by the provisions.
<p>Official Secrets Act (1923) ¹⁰⁶</p> <p>Key Provisions of Concern:</p> <ul style="list-style-type: none"> – s3C: Authorises imprisonment for up to 14 years for anyone who, “<i>for any purpose prejudicial to the safety or interests of the State... obtains, collects, records or publishes or communicates to any other person any...article or note or other document or information which is calculated to be or might be or is intended to be, directly or indirectly, useful to an enemy.</i>”

¹⁰⁴ [Myanmar Penal Code](#) (1957).

¹⁰⁵ [Myanmar Emergency Provisions Act](#) (1950).

¹⁰⁶ [Myanmar Official Secrets Act](#) (1923).

E. Guidance for Governments and ICT Companies on Meeting International Standards

Table 22: Guidance for Governments on ICT Policy and Law Making

- UN Special Rapporteur on Freedom of Opinion and Expression – [Report on Freedom of Expression and Opinion on the Internet](#) (2011)
- Representative on Freedom of the Media of the Organisation for Security and Co-operation in Europe (OSCE) – [Report on Freedom of Expression on the Internet](#) (2011)
- International Mechanisms for Promoting Freedom of Expression – [Joint Declaration on Freedom of Expression and the Internet](#)
- International Mechanisms for Promoting Freedom of Expression – [Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation](#)
- Parliamentary Assembly of the Council of Europe – [Resolution 1577](#)
- [International Principles on the Application of Human Rights to Communications Surveillance](#) (2013)
- UN Special Rapporteur on Freedom of Opinion and Expression – [Report on Surveillance of Communications](#) (2013)
- World Summit on the Information Society – [Declaration of Principles](#) (2003)
- Internet Rights & Principles Dynamic Coalition – [Internet Rights & Principles Charter](#)

Table 23: Guidance for ICT Companies on Meeting International Standards

- Telecommunications Industry Dialogue – [Guiding Principles on Freedom of Expression and Privacy](#) (2013)
- Global Network Initiative – [Implementation Guidelines](#) (2010)
- Access – [Telco Action Plan](#) (2011)
- UN Special Rapporteur on Freedom of Opinion and Expression – [Report on Freedom of Expression and Opinion on the Internet](#) (2011)
- UN Special Rapporteur on Freedom of Opinion and Expression – [Report on Surveillance of Communications](#) (2013)