Executive Summary & Recommendations

EXECUTIVE SUMMARY

The roll-out of new information and communications technologies (ICT), infrastructure and services in Myanmar is having a transformative impact on the country. Mobile phone penetration has increased from 7% to 33% between 2012 and 2014, and continues to rise. The growing availability of smartphones is increasing opportunities for Internet access. It has been estimated that by 2030 the ICT sector could contribute $6.4 billion to Myanmar's GDP and employ approximately 240,000 people.

The ICT sector is having a transformative impact on Myanmar at the same time as the country itself is undergoing a transformation: emerging from decades of ethnic-based armed conflict, authoritarian rule and economic isolation. Myanmar is – and will remain for some time – a high-risk country with poor governance. The headlong rush to improve access to ICTs brings challenges, particularly in the absence of adequate policy and legal frameworks. These frameworks are lacking both for the rollout of the network and other services, and for considering and controlling wider impacts on society associated with greater use of ICTs, such as surveillance of communications and "hate speech" online. The gaps in the policy and legal frameworks are compounded by people's basic lack of experience of using ICTs, resulting in the potential for misuse and negative impacts on a range of human rights, particularly the rights to privacy and freedom of expression.

This means that conducting business responsibly in Myanmar's ICT sector requires a clear commitment to understanding the complex operating context and its constraints to determine what impacts business activities may have on people in Myanmar. This needs active engagement by companies, Government and civil society to promote public and informed debates, which are still a rarity in Myanmar. This also includes the need for robust approaches to filling in the gaps by managing negative impacts in line with international standards on responsible business conduct.

This Sector Wide Impact Assessment (SWIA) carried out by the Myanmar Centre for Responsible Business (MCRB), in partnership with its co-founders, the Institute of Human Rights and Business (IHRB) and the Danish Institute of Human Rights (DIHR) is focused on Myanmar's ICT sector. It is based on both desk-based and field research in Mandalay, Sagaing and Yangon Regions, and Shan, Mon and Kayin States. It includes in-depth analysis of existing Myanmar policy and legal frameworks relevant to the sector, as well as the historical, political and economic context. It also includes research on the policies and practices of a wide range of companies in the ICT sector in Myanmar in order to further understanding and set out an analysis of the sector and its actual and potential impacts on Myanmar society.

The idea behind a SWIA is to present key human rights risks and opportunities for the Government of Myanmar, companies operating in the sector, and civil society in order to improve the regulation and operations of the sector in a manner that provides benefit to

Myanmar, its people, and businesses. It is a forward-looking assessment that aims to contribute to preventing and minimising the sector's negative impacts as well as strengthening and improving the sector's positive impacts (See Chapter 1 for more detailed information on the purpose and methodology behind the SWIA).

Key Actors in the ICT Sector

Government of Myanmar

As with other sectors in Myanmar, the Government departments overseeing the ICT sector are reliant on a small group of overworked civil servants. Few have the technical capacity to pursue the Government's ambitious "e-agenda" of providing citizens with access to technology to help Myanmar accelerate its development and move from isolation to global connectivity and competition. The challenges of developing the sector are enormous – from planning the expansion of network infrastructure and services, to establishing appropriate technical standards for emerging platforms, to reinvigorating an education system for the 21st century. The ICT sector is innately interconnected, bringing with it a host of challenges in addressing international standards and international relations that are inherently foreign to a formerly long-isolated country. Development partners such as the World Bank and Asian Development Bank are, however, supporting with technical assistance, as demonstrated by the transparent process for awarding the telecoms licences in 2013.

Yet technical assistance is no substitute for Myanmar Government staff grappling with the day-to-day challenges themselves. This includes a legal framework that is not designed for the modern technological age, nor aligned with international standards that were of little interest to earlier military governments. The legacy from that era that is enshrined in laws intended to restrict communication and sits uneasily with a burgeoning sector that exists, in many ways, to do the opposite. The challenge of updating the policy and legal frameworks to keep pace with technological developments and stay in line with the Government's ambitious reform programme is matched by the far less visible, but no less significant, challenge of reorienting both the authorities' and people's mindsets towards governance based on openness, transparency and accountability. This SWIA seeks to highlight the significant gaps in policy and laws that should be addressed as part of the Government's policy and legal reform process.

Companies in the ICT Sector

As in other countries, there is great variability amongst the companies in the sector, from local start-ups to large multinationals. Unlike tech start-ups in other countries, small local companies have not often been exposed to key global debates in the sector, nor access to content in their own languages. The learning curve is therefore likely to be steep, not only in meeting expectations of international business partners, but also in understanding the need for and approach to key issues like protection of data and, importantly, international standards on responsible business.

The rush to expand the network means that many companies and their local subcontractors are learning on the job. Some bring with them established governance, health, safety, environment and labour compliance frameworks and monitor them with spot checks, while others do not operate any systematic safety procedures. The human rights impacts observed during the research were in some cases quite visible, particularly in tower construction and laying fiber, including safety violations and in some cases extremely poor working conditions. The short-term employment opportunities for unskilled workers and semi-skilled workers provide much sought after jobs. However, they are often temporary, and sometimes involve harsh working conditions and piecemeal pay. In the longer term, the sector offers many job opportunities, but the skills and capacity needs to be built among the workers required to fill them.

The competitive forces driving the market, such as the rush to rollout mobile phone networks, can also counteract the incentives that exist to apply responsible business standards in Myanmar. Research for this SWIA started in July 2014, when the operators were rolling out and launching their new networks under severe time pressure. However, some of the larger operators have their own standards of conduct, which can drive responsible business practice more widely in the sector, if they are willing and able to apply them robustly in such challenging circumstances. Lessons learned from international initiatives that address some key challenges in respecting human rights in the ICT sector can also be useful for Myanmar. This SWIA aims to highlight the risks, and capture some of those demonstration effects and lessons learned across a range of topics relevant to the operation of the sector.

Civil Society

The research also showed that very few civil society groups, human rights defenders or media organisations had an understanding of the sometimes complicated and technical human rights issues associated with the ICT sector. The SWIA is also intended to raise wider awareness among these groups.

Users and Communities

The research also revealed a hunger and enthusiasm for mobile phone connectivity and Internet access, with a rapid uptake of social media services in particular. But it also revealed little user awareness of either the risks that the ICT sector can bring to them or the wider opportunities for the country. Digital literacy is extremely low in Myanmar. This is compounded by the novelty of the concept of privacy as understood in international laws and standards. In a country with a limited concept of physical privacy, promoting the concept of digital privacy and data protection among users is critical.

As with other SWIAs carried out by MCRB, IHRB and DIHR, observable company engagement and two-way communication with communities and workers was lacking, particularly in association with the network roll-out. This is particularly important in ethnic minority areas, including those affected by conflict, where it is essential to take the time to engage directly with as wide a range of stakeholders as possible. It addition to building a more complete picture of the conflict and inter-communal dynamics, it enables companies to understand what concerns or questions local people may have about the introduction of

ICTs. The potential for the on-going conflicts in certain ethnic areas to block, delay or sabotage further roll out could lead to a deepening of the digital divide, reinforcing inequality in conflict areas unable to access and benefit from ICTs.

Five Main Themes Emerge from the ICT SWIA

- **Gaps in the policy, legal and regulatory framework:** Modern laws do not exist for most of human rights risks posed by the ICT sector in Myanmar, and in particular lawful interception, data privacy, access to information, certification bodies, cybersecurity, data protection and cybercrime. Myanmar needs to fill the regulatory gaps through a rights-based approach which learns from good (and bad) practice elsewhere.

- **Access:** There is an opportunity to create an investment climate that supports an extensive telecommunications network and strong competition to bring down prices and achieve universal access and accessibility of ICTs. It is important to include local languages and standardised Unicode fonts that allow full searchability and access to information. This will ensure that the whole country can enjoy the social and development benefits inherent in positive technological development and global connectivity.

- **Online "Digital Dangers":** With the benefits of greater access to modern technology and the Internet come certain risks and digital dangers. These include risks to data privacy, various forms of cybercrime, including child sexual abuse images and revenge porn, cyberbullying and stalking, and "hate speech". Other digital dangers include the wider consequences of Government-ordered mobile and Internet network shutdowns and the selective blocking of websites. Companies, Government and the media need to educate the public about these issues. They should highlight safe behaviours (such as encryption or not posting or emailing personal information) through Burmese and other local language communications including software and application agreements, media articles, and other channels.

- **"Offline" human rights issues:** Complex land laws and processes for granting land use to erect telecoms towers are just one of the many problems faced by the Government, communities, operators and their subcontractors regarding the national network rollout. Rapidly changing labour laws and low awareness of rights means workers, and in some cases employers, are not well informed about even the most basic labour rights protections. While that function is often filled by trade unions in other countries, in Myanmar independent unions are only just emerging after many years of prohibition and are therefore new to these issues. The forced labour previously associated with the last military government is now generally limited to conflict areas, but new forms of forced labour are emerging in the private sector. One such example found in the research were workers required to work for a businessman to pay off work-related debts. Corruption in the permitting process is also a risk around network rollout.

- **Exacerbating or addressing visible divisions in society**: ICT has the potential to be used to impact positively or negatively on the rights of groups at risk**,** such as children. While there are gradual improvements in some areas of discrimination, religious discrimination and related violence is a serious problem and in recent times particularly impacting the Muslim community. The research and other reports have identified disturbing patterns of anti-Muslim “hate speech” on social media in particular. Yet ICTs also have the potential to improve the situation of some groups at risk, such as people living with disabilities, by providing them with services or income generation opportunities from which they were previously excluded. There are also more female than male graduates in ICT related study, opening potential new areas of employment for women.

Issues on the horizon

With little to no in-country manufacturing, and a desire for even the most basic, second-hand phones, problems seen in other countries with e-waste or environmental pollution have yet to emerge in Myanmar. They will doubtless do so in time. Due to the absence of manufacturing, the SWIA does not cover “conflict minerals” such as gold, tin, tungsten and tantalum, although the first three are all produced in Myanmar. Research on how these minerals are being produced and sold and their relation to on-going conflicts in the country would be a useful topic for further investigation.

Recommendations

These Recommendations build on the measures expected of governments and businesses under the UN Guiding Principles on Business and Human Rights. Governments have a duty to protect human rights and all businesses – Myanmar and foreign – in the ICT value chain have a responsibility to respect human rights. Key excerpts from the UN Guiding Principles are highlighted in boxes at relevant points below. Further global human rights guidance for the ICT sector is available from European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights" (2013).

Recommendations To the Government of Myanmar

1. Establish a coherent policy framework for the ICT sector with adequate safeguards.

UN Guiding Principles on Business and Human Rights: The State Duty to Protect

1. States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication.

2. States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations.

The Government has embraced the importance of providing citizens with open access to technology and has also committed to a "people-centred" approach to development. A balanced approach that stimulates the spread and uptake of ICTs services while protecting the rights and interests of the population will be required to realise the positive potential of the ICT sector for Myanmar society. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

Key Points for Implementation

- **Include adequate human rights, environmental and social safeguards for private sector operations in the forthcoming Master Plans for the ICT Sector.** These include the ICT Master Plan, the E-Governance Master Plan, and the Telecommunications Master Plan. Suggested safeguards are highlighted at the end of each SWIA Chapter. In addition, each Masterplan should be underpinned by a commitment to **advancing government transparency, accountability and public participation**. As part of that commitment, the government should engage in open, public and meaningful consultations on the Master Plans leaving sufficient time for stakeholders to comment. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

- **Undertake ongoing identification, prevention and mitigation of the potential longer-term and cumulative human rights, environmental and social impacts** when developing new strategic directions for the ICT sector. This could apply to further development of ICT parks, increased manufacturing, or developing outsourcing services. The aim should be to avoid and reduce the potential longer-term and cumulative negative impacts. (See Chapter 5 on Cumulative Impacts for further information). The government should also consider and plan for the predictable **environmental impacts** of the sector, in particular **e-waste** generated by the disposal of ICT equipment.
- Complete the transformations at the Ministry of Communications and Information Technology (MCIT) to establish the Post & Telecommunications Department (PTD) as **an independent ICT regulator** and Myanmar Post and Telecommunication (MPT) as **a privatised telecommunications operator and Internet service provider (ISP).**

2. Improve ICT-specific legal and regulatory reforms to ensure appropriate safeguards around Government activities and a coherent framework for responsible business conduct in the ICT sector.

UN Guiding Principles on Business and Human Rights: State Regulatory and Policy Functions

3. In meeting their duty to protect, States should:

a) Enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, and periodically to assess the adequacy of such laws and address any gaps;

b) Ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights;

c) Provide effective guidance to business enterprises on how to respect human rights throughout their operations;

d) Encourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts.

UN Guiding Principles on Business and Human Rights: Ensuring Policy Coherence

8. States should ensure that governmental departments, agencies and other State-based institutions that shape business practices are aware of and observe the State's human rights obligations when fulfilling their respective mandates, including by providing them with relevant information, training and support.

Myanmar has embarked on an ambitious programme of legal and regulatory reforms across the board, including changes specifically focused on the ICT sector. An appropriate legal framework can protect the rights of the population and encourage responsible business conduct. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

Key Points for Implementation

- Ensure forthcoming regulations under the *Telecommunications Law*, *Computer Science Development Law* and *Electronic Transactions Law* confirm that **criminal penalties cannot be applied for legitimate expression**.
- The regulations should also **clarify the procedures and safeguards for blocking or filtering content** in line with international human rights standards. Any takedown requests should target specific pieces of content, rather than access to whole domains.

- **Clarify and limit the *Telecommunications Law* provisions on telecommunications network shutdowns** in line with international standards**.** A suspension of telecommunication services (mobile and/or landline) must be prescribed by law and only invoked if there is a real and imminent threat to national security or a national emergency. There must be a clear and transparent process around who is authorised to make a shutdown request, it should be limited in geography, scope and duration, and should be publicly reported after the fact. Network shutdowns affecting the whole country should never be authorised.
- **Make a commitment not to shut down the network during the upcoming elections.** Instead put in place plans to deal with potential emergencies, such as appropriate restrictions on the circulation of mass messages inciting violence and hate speech.
- **Introduce regulations on protecting data privacy** in line with international standards.
- **Mandate clear data protection and security standards** for entities licensed to provide mobile money services and other online services.
- **Consider alternative options to mandatory SIM card registration** given the potential chilling effects on freedom of expression.
- **Do not prevent companies from reporting** on the nature and number of **requests they receive from the Government of Myanmar** for lawful interception, communications data, content removal or blocking of websites, or requests for network shutdowns.

3. Improve wider legislative and regulatory reforms on freedom of expression and association, land use and management and labour issues to ensure appropriate safeguards around Government activities and a coherent framework for responsible business conduct in the ICT sector.

There are a wider range of laws that affect the ICT sector and users in Myanmar, many of which are part of the Government's ambitious programme of legal and regulatory reforms. As with the ICT-specific laws, these reforms should encourage further ICT development but in a way that protects the rights of the population and encourages responsible business conduct. (See Chapter 2 on ICT Government Institutions, Policies & Legal Frameworks for further information).

Key Points for Implementation

Freedom of Expression and Association:

- **Amend the *Law Relating to Peaceful Assembly and Peaceful Procession* to eliminate the criminalisation of protests and demonstrations,** which are increasingly taking place using ICTs.
- **Amend key laws restricting the right to freedom of expression**, including *1908 Unlawful Associations Law*, *1950 Emergency Provisions Act*, *1923 Official Secrets Act*, and various articles of the *Penal Code*, especially *Article 505(b)*.
- **Fully implement *Articles 3* and *4* of the *2014 Media Law*,** which provide for **"freedom from censorship"** and freedom to criticise the Government. Ensure that the media, including online journalists, are able to perform their legitimate functions without fear of censorship or arrest.

See Chapter 4.1 on Freedom of Expression for further information.

Labour:

- **Develop a comprehensive and overarching labour law framework** in line with international labour standards. Extend protection to all types of workers, including temporary and migrant workers. Given the expected expansion of employment in the ICT sector, and the competition to retain skilled Myanmar nationals, reinforcing the Government's commitment to the ILO's programme on Decent Work will be an important signal to workers and to ICT sector employers.
- **Strengthen the protection of workers involved in trade union activities** to ensure that they do not face discrimination or dismissal by employers solely for their legitimate trade union activities. Support trade unions to operate at the sector level so that they can adequately represent workers, including in growing sectors such as ICT where an increasing number of workers are expected to be employed. Raise awareness among employers with more than 30 workers about the legal requirement to put in place a workplace coordinating committee.
- **Demonstrate that the Government is committed to gender equality** by encouraging the employment of the large number of female graduates in ICT related studies, on the basis of equal pay for equal work.
- **Task labour inspectors with targeting their visits to high-risk sites,** such as tower construction and fibre trenches.

See Chapter 4.6 on Labour for further information.

Land Use and Management:

- **Ensure the forthcoming National Land Use Policy reflects the customary, informal and communal land ownership and use** arrangements in Myanmar, both in terms of protecting security of tenure and ethnic minority rights.
- **Establish a coherent legal framework for land use in line with international standards** (such as the FAO Voluntary Guidelines on the Responsible Governance of Tenure of Land, Fisheries and Forests in the Context of National Food Security) for private sector operations within the forthcoming comprehensive land law. This should ensure the protection of existing use and ownership rights while providing certainty and clarity around permitted transactions. This includes reforming existing land dispute mechanisms to enable enforcement of resolutions relating to land.
- **Clarify and simplify land classification and use procedures** to provide appropriate protection for farmers from unscrupulous land transactions and for food security. These should be sufficiently flexible to allow farmers to pursue alternative livelihood options on a portion of their land (such as leasing it for telecom equipment) and/or encourage local entrepreneurship.
- **Encourage telecommunications operators to follow the World Bank's** Myanmar Telecommunications Environmental and Social Management Framework and Land Lease Guidelines, including requiring their subcontractors to follow these guidelines in all land dealings.
- **Promote the sharing of tower infrastructure** to limit the impact on land take and improve efficiency.

See Chapter 4.7 on Land for further information.

Groups at Risk:

- Develop a more comprehensive framework for **child protection**, including relevant provisions for child safety online. The Government should consider asking companies and other governments to share expertise and good practices from other jurisdictions.
- Consider including **protections for women against online harassment** in the forthcoming law on violence against women.

See Chapter 4.8 on Groups at Risk for further information.

4. Adopt a rights-respecting lawful interception model and maintain open access to the Internet to ensure Myanmar does not become a modern "surveillance state".

UN Guiding Principles on Business and Human Rights: The State-Business Nexus

5. States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may impact upon the enjoyment of human rights.

6. States should promote respect for human rights by business enterprises with which they conduct commercial transactions.

The Government has previously used ICTs to conduct surveillance of its citizens, both within the country and abroad. A modern legal framework limiting Government surveillance is overdue. (See Chapter 4.4 on Surveillance for further information).

Key Points for Implementation

- Follow through on the Government's stated commitment to **align the forthcoming lawful interception regulations or framework to international human rights standards.** See the **Annex to the Recommendations** for key considerations for each step of the interception process that should be incorporated into the forthcoming regulations. As it has with other draft ICT laws and regulations, MCIT should make any draft regulation or framework on lawful interception available for public comment for at least three weeks, and widely publicise the consultation process.
- **Publicly commit to prohibit "mass surveillance**" (commonly understood to refer to the bulk access and/or collection of many users' communications without prior suspicion of criminal activity). Such a commitment should also be incorporated into the forthcoming lawful interception regulation or framework (which should authorise only targeted interception where there is a prior suspicion of recognisably criminal activity).
- **Refrain from purchasing and utilising invasive and often unregulated communications surveillance technology** to carry out communications surveillance. Once Myanmar intelligence agencies have such capabilities, it will be much more difficult to eliminate or regulate their use. It is important for the Government, and the ICT companies that may be subject to lawful intercept orders, to make the distinction between software and other tools that comply with international standards on lawful interception, and products that fall below international standards because they are unregulated and pose a risk to human rights.

5. Improve data protection standards and cybersecurity.

Myanmar currently does not have any requirements or standards on data protection for companies. A failure to protect people's personal information and identity can pose significant risks to the right to privacy and security. As Myanmar puts in place its *cybersecurity infrastructure, and the laws and regulations underpinning it, it will be important to balance the legitimate need to combat cybercrime with human rights protections. (See Chapter 4.5 on Cybersecurity for further information).*

Key Points for Implementation

- **Establish clear standards of data protection for companies and other organisations collecting, storing, or sharing user data.** This includes standards around data privacy, requirements to make privacy policies publically available, prior informed consent for the use of data and grievance mechanisms for users, and baseline security standards.
- **Promote awareness of the importance of cyber security for users** and build digital literacy through clear and concise communication. Widely disseminate basic best practices for users in partnership with the **Myanmar Computer Emergency Response Team (MMCERT).**
- **Do not criminalise the use of encryption tools by individuals.** Encryption is essential, not just for security of transactions but also the safety of human rights defenders. Blanket prohibitions on encryption, and therefore anonymity of communications, are not a necessary and proportionate response in line with international human rights standards.
- **Consider establishing a National Data Protection Authority** that would be in charge of the protection of data and privacy and that can handle complaints from users.

6. Demonstrate a commitment to free and open communication through a modern Freedom of Information law and build meaningful transparency systems across Government.

The Government has made a welcome commitment to join the Open Government Partnership and to modernise its approach to governance through its e-Governance Master Plan. It will be important to embed protections around the right to privacy into e-governance approaches so that they are trusted and can become a driver for ICTs and innovation. (See Chapter 4.1 on Freedom of Expression for further information).

Key Points for Implementation

- **Adopt a modern Freedom of Information Act**, as part of other steps towards **transparency** (e.g. commitments to join the Open Government Partnership by 2016, candidacy for Extractives Industries Transparency Initiative, and conducting more transparent licensing processes). If the **Constitution** is to be amended, include constitutional guarantees of public access to information held by the Government.
- Ensure that **privacy/data protection requirements** and safeguards are embedded into e-governance and open data initiatives.
- **Commit to access to information requirements that are aligned with the Open Government Partnership Principles**: the publication of all government-held information (which is broader than information only on government activities); proactive and reactive releases of information; mechanisms to strengthen the right to information; and open access to government information.
- **Commit to implementing core open data principles**, including across on-going national e-governance projects, such as the Common Citizen Service Data Portal to be

developed by MCIT and the World Bank. Given the increasing prevalence of mobile phones, ensure Government data displays are user-friendly and mobile-friendly.

- **Consult publically with civil society and business to identify high-value data** that catalyses innovation, enhances social policy, and promotes public and private sector accountability.

7. Accelerate the implementation of Myanmar's universal service commitments.

Until recently, Myanmar was at the bottom of the global league table for Internet and mobile phone penetration. While penetration rates are increasing rapidly, it may take years to reach all of Myanmar's population, particularly in rural areas. The Government tentatively committed to a universal service agreement with the current telecommunications operators, which called for each operator to contribute 2% of annual revenue to a universal service fund managed by MCIT, beginning after three years of successfully meeting network rollout targets. Myanmar has also joined the Alliance for Affordable Internet (AFAI). All parties can play a role in accelerating the roll out of services using innovative solutions so that a wider percentage of the population benefits from accessing ICTs. (See Chapter 3 on Sector Impacts for further information).

Key Points for Implementation

- **Publically disclose the current national rollout requirements for operators,** compared with their current progress.
- Build on lessons learned in the World Bank supported programme of **extending connectivity to rural areas**.
- **Develop a Universal Service Strategy,** as a first step in the implementation of Chapter XV of the *2013 Telecommunications Law*. **Consult widely**, including with ethnic minorities and disadvantaged groups such as people with disabilities, to identify priority areas for the rollout of telecommunications service (both mobile and fixed line broadband service), for inclusion in the Universal Service Strategy and Fund.
- Clarify how the Universal Service Fund will support **Myanmar's commitment to the Alliance for Affordable Internet,** which is focused on realising entry-level broadband priced at less than 5% of monthly income, particularly in rural communities
- **Consider allocating Universal Service Funds to support community-based telecommunications networks** and provide wireless spectrum concessions to remote rural communities where telecommunications service is currently inaccessible. This will help promote the development of low-cost community-based telecommunications networks for last mile or last inch connectivity.

8. Improve digital literacy of users and send clear signals about respectful use of ICT's.

To realise the range of transformative positive impacts via ICT growth and development in Myanmar, the Government must ensure that all Myanmar's population can participate in Myanmar's growing information society. Those services must be used respectfully so that violence and discrimination happening offline are not magnified and intensified online. This requires strong signals from opinion-formers, including Government. Engagement with ICTs is still a completely new experience for the majority of Myanmar people. *There is also a need for efforts from Government, business and civil society to provide* *awareness and training on protection against threats. (See Chapter 3 on Sector-level Impacts and Chapter 4.3 on Privacy for further information).*

Key Points for Implementation

- **Ensure ICTs are "localised" for Myanmar users,** meaning technologies and content, including data and text, are adapted to support the wide range of languages in Myanmar, in addition to Burmese. The Government should commit to supporting the development of hardware, software, education materials, user manuals, amongst others, in all the main languages of Myanmar.
- **Support awareness raising campaigns and training around online safety and behaviour, including child safety**.
- **Send clear public signals from the highest level of government and all political parties that "hate speech" is unacceptable.** Hate speech spreads quickly online and has been used to incite violence. The Myanmar Government should actively support efforts aimed at "counter speech", where users challenge "hate speech" for example, by exposing false rumours, ideally with the support of the police, and encouraging peaceful expression.
- **Prioritise public education sector reforms that include a modernised ICT curricula for higher and vocational education** to meet the needs of employers.

9. Strengthen requirements for responsible business conduct in the ICT sector, including by requiring companies to provide operational grievance mechanisms for anyone impacted by their activities, and to report on their implementation.

UN Guiding Principles on Business and Human Rights: Access to Effective Remedy

25. As part of their duty to protect against business-related human rights abuse, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy.

UN Guiding Principles on Business and Human Rights: Operational Grievance Mechanisms

29. To make it possible for grievances to be addressed early and remediated directly, business enterprises should establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted.

UN Guiding Principles on Business and Human Rights: Effectiveness criteria for non-judicial grievance mechanisms

31. In order to ensure their effectiveness, non-judicial grievance mechanisms, both State-based and non-State-based, should be:
(a) Legitimate: enabling trust from the stakeholder groups for whose use they are intended, and being accountable for the fair conduct of grievance processes;
(b) Accessible: being known to all stakeholder groups for whose use they are intended, and providing adequate assistance for those who may face particular barriers to access;
(c) Predictable: providing a clear and known procedure with an indicative time frame for each stage, and clarity on the types of process and outcome available and means of monitoring implementation;
(d) Equitable: seeking to ensure that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair, informed and respectful terms;
(e) Transparent: keeping parties to a grievance informed about its progress, and providing sufficient information about the mechanism's performance to build confidence in its effectiveness and meet any public interest at stake;
(f) Rights-compatible: ensuring that outcomes and remedies accord with internationally recognised human rights;
(g) A source of continuous learning: drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms;

Recs

> *Operational-level mechanisms should also be:*
> *(h) Based on engagement and dialogue: consulting the stakeholder groups for whose use they are intended on their design and performance, and focusing on dialogue as the means to address and resolve grievances.*

The Government should clearly signal its expectations to companies (foreign or local) that it expects responsible investment aimed at the long-term interests of Myanmar and all of its people. That expectation can be expressed in policies and law (see Recommendations to the Government of Myanmar, numbers 2 and 3, above). It can be strengthened through public awareness raising and capacity building of Myanmar companies, and by ensuring that they make themselves accountable to the population (see Recommendations to Companies below). As Myanmar's judicial system reforms will take many years, in the interim, it is important that effective alternatives to formal legal proceedings are available to ensure that access to remedy is readily available to those adversely impacted by business activities.

Key Points for Implementation

- **Set out the Government's expectation that businesses investing and doing business in Myanmar will engage in responsible business conduct,** whether through enterprise registration or through a permit from the Myanmar Investment Commission (MIC). This could for example be through public guidance from the Directorate of Investment and Companies Administration (DICA) to all Myanmar and foreign companies.
- **Include two contractual terms relating to responsible business in MIC Permits, requiring**:
  - An annual report explaining the company's approach and outcomes in conducting business responsibly
  - All companies granted a MIC permit should establish mechanisms to receive and constructively address concerns and complaints, from workers, communities and civil society, consistent with the effectiveness criteria of principle 31 of the UN Guiding Principles on Business and Human Rights

Recommendations
To ICT Companies

1. Apply international standards of responsible business conduct in the absence of developed national legal frameworks, in particular the UN Guiding Principles on Business and Human Rights.

UN Guiding Principles on Business and Human Rights: The Corporate Responsibility to Respect

10. Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

UN Guiding Principles on Business and Human Rights: Human Rights Policy Commitment

15. In order to meet their responsibility to respect human rights, business enterprises should have in place policies and processes appropriate to their size and circumstances, including:

a) A policy commitment to meet their responsibility to respect human rights;

b) A human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights;

c) Processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.

UN Guiding Principles on Business and Human Rights: Human Rights Due Diligence

17. In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. Human rights due diligence:

a) *Should cover adverse human rights impacts that the business enterprise may cause or contribute to through its own activities, or which may be directly linked to its operations, products or services by its business relationships;*

b) *Will vary in complexity with the size of the business enterprise, the risk of severe human rights impacts, and the nature and context of its operations;*

c) *Should be ongoing, recognising that the human rights risks may change over time as the business enterprise's operations and operating context evolve.*

This SWIA has highlighted the current gaps in the Myanmar's evolving policy and legal framework. Due to the rapid pace of change, and lack of capacity and experience among legislators and Government ministries, there is no guarantee that, once adopted, Myanmar laws will fully reflect international standards. Nor are they guaranteed to protect workers, users, communities and the businesses themselves from the risks highlighted in the SWIA. In addition to providing companies certainty at a time when the national legal landscape is in flux, using international standards – such as the UN Guiding Principles on Business and Human Rights (and the OECD Guidelines on Multinational Enterprises for the companies to which they are applicable) – also provides confidence to local and international stakeholders. Because the situation is changing so rapidly, ICT sector companies should consistently scan their operating environments to understand the human rights risks that may be created by Government actions, or by their own operations, or those of their business partners.

Key Points for Implementation

- **Adopt a policy commitment to respecting human rights**, and ensure it is embedded across the company and widely communicated to stakeholders. Such a public commitment is important because it demonstrates that top management consider respect for human rights as a minimum standard to conduct business with legitimacy. A few Myanmar companies have begun to adopt human rights commitments and publicly report on implementation.[1] Such commitments signal to local stakeholders a break with the past. To international business partners they signal an awareness of, and commitment to, operating in accordance with international standards.
  - **Ensure other operational policies and processes** are aligned with the human rights commitment, for example, **clear and accessible privacy policies** that explain the company's policy on protection and its use or sale of customer's data. For ICT companies that interact directly with users or customers, the company's **Terms of Service, "user community" guidelines or similar documents**, should explain the use of the company's services in clear and accessible language, including in Burmese and other local languages.
- **Carry out human rights due diligence on an on-going basis:**
  - **Assess the risks and impacts the company and the other companies in its value chain** (suppliers, contractors, etc) **could pose to people and their human rights**.
    - Take account of local complexities and legacies, including **the considerable gaps in the existing legal framework** identified in the Recommendations to the Myanmar Government, numbers 2 and 3 (and throughout this SWIA). Seek to fill those gaps by operating according to international standards. Take account of **conflict dynamics** when operating in areas of latent, existing and potential armed conflict.
    - **Explicitly consider** risks of contributing to or being directly linked to Government or business partners' actions that may violate human rights. This should go beyond simply ensuring that business partners are not, nor have been, on the US or other sanctions list. Given the past involvement of some businesses in government or military related human rights abuses, careful due diligence is necessary including around the company's commitment to responsible business practice, transparency and international standards.
  - Use the assessment of potential risks **to identify and implement steps to prevent or at least mitigate those risks.** The types of actions will vary considerably. It might include taking collective action to work with the Government to address gaps in the laws (see Recommendation 5 below), or specific actions in conflict-affected areas. See Recommendation 3 below on the wide range of risks and suggested responses highlighted in the SWIA.
  - **Track responses to identified risks and impacts**. Consider how workers, communities, users, customers and others potentially affected by company operations can be involved in monitoring activities.
  - **Communicate publicly about** what the company is doing to address the human rights impacts raised in this SWIA and more broadly, particularly when concerns

[1] Pwint Thit Sa/Transparency in Myanmar Enterprises Report (2015) is intended to encourage increased transparency by Myanmar businesses by rating them based on information they publish on the internet in the areas of anti-corruption, organisational transparency, and human rights, health, safety and the environment.

are raised by affected stakeholders, as recommended in MCRB's Pwint Thit Sa/TiME project.

- Proactively **report on the requests received from the Myanmar Government** (at all levels) for lawful interception, communications data, content removal and website blocking, and requests for network shutdowns, in order to stimulate further transparency around what the Government is asking companies to do and how companies are responding.
- **Make it easier for Myanmar users to communicate with the company** by providing services in local languages and offering services that come pre-loaded with Myanmar fonts.
- **Focus on simply and clearly communicating risks** to users (such as through graphic icons), including terms of service, privacy policy etc.

2. Incorporate the thematic risks and recommendations presented throughout this SWIA into company operations and interactions.

The Recommendations in this section reflect a set of cross-cutting and overarching actions to ensure responsible business conduct in Myanmar's ICT sector. In addition, each of the ten sections in Chapter 4 include specific thematic recommendations that provide more detailed considerations that companies should consider in their on-going human rights due diligence, operations and actions.

Key Points for Implementation

See the specific recommendations from Chapter 4:

- Chapter 4.1: **Freedom of Expression & Opinion** Recommendations for ICT Companies
- Chapter 4.2: **Hate Speech** Recommendations for ICT Companies
- Chapter 4.3: **Privacy** Recommendations for ICT Companies
- Chapter 4.4: **Surveillance** Recommendations for ICT Companies
- Chapter 4.5: **Cyber-Security** Recommendations for ICT Companies
- Chapter 4.6: **Labour** Recommendations for ICT Companies
- Chapter 4.7: **Land** Recommendations for ICT Companies
- Chapter 4.8: **Groups at Risk** Recommendations for ICT Companies
- Chapter 4.9: **Stakeholder Engagement & Grievance Mechanisms** Recommendations for ICT Companies
- Chapter 4.10: **Conflict & Security** Recommendations for ICT Companies

3. Engage with potentially affected stakeholders, particularly workers, communities, customers and users, to build trust and demonstrate transparency and accountability.

Engagement cuts across many recommendations concerning improved human rights practices by companies, and is integral to their success. Sincere, on-going two-way engagement with workers, workers' representatives, users and communities is one of the most valuable things a company can do to prevent and mitigate risk, particularly in the Myanmar context where there has historically been a lack of trust of companies by communities and others.

Key Points for Implementation

- **Proactively undertake ongoing and meaningful engagement** with workers, their representatives, users and communities throughout the project lifecycle, including at early stages of activities and key operational moments where risks change, recognising that engagement is a new concept for many in Myanmar. For example, Myanmar labour law requires an employer with more than 30 workers to form a Workplace Coordinating Committee (2 representatives of workers, 2 representatives of employer) whether or not there is labour organisation (e.g. union) in the enterprise. This kind of joint committee provides the outlet for mutually beneficial joint monitoring of working conditions by workers and the enterprise.
- **Provide basic information to users and customers about how to stay safe online** by protecting personal data, and support digital literacy growth for users, including the need to manage their "digital footprint" across devices and services and reporting concerns.
- **Proactively provide information in a variety of formats** and understandable local language(s) on key issues that are of concern to the Myanmar public, such as the health and safety impacts of mobile phones and cell towers.
- **Online consultation and communication is nascent in Myanmar**, but webchats could be a form of communication with stakeholders who are increasingly expecting to access responses from companies via their Facebook pages.

4. Put in place mechanisms that can address concerns and grievances quickly and effectively.

UN Guiding Principles on Business and Human Rights: Remedying Impacts

22. Where business enterprises identify that they have caused or contributed to adverse impacts, they should provide for or cooperate in their remediation through legitimate processes.

UN Guiding Principles on Business and Human Rights: Effectiveness Criteria

31. In order to ensure their effectiveness, non-judicial grievance mechanisms, both State-based and non-State-based, should be:
(a) Legitimate: enabling trust from the stakeholder groups for whose use they are intended, and being accountable for the fair conduct of grievance processes;
(b) Accessible: being known to all stakeholder groups for whose use they are intended, and providing adequate assistance for those who may face particular barriers to access;
(c) Predictable: providing a clear and known procedure with an indicative time frame for each stage, and clarity on the types of process and outcome available and means of monitoring implementation;
(d) Equitable: seeking to ensure that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair, informed and respectful terms;
(e) Transparent: keeping parties to a grievance informed about its progress, and providing sufficient information about the mechanism's performance to build confidence in its effectiveness and meet any public interest at stake;
(f) Rights-compatible: ensuring that outcomes and remedies accord with internationally recognised human rights;
(g) A source of continuous learning: drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms;

Operational-level mechanisms should also be:
(h) Based on engagement and dialogue: consulting the stakeholder groups for whose use they are intended on their design and performance, and focusing on dialogue as the means to address and resolve grievances.

There are few outlets in Myanmar for effective resolution of grievances either through judicial or non-judicial means. This makes company-based alternatives all the more important to ensure issues are identified early and addressed quickly before they *escalate. One of the most efficient ways for a company to remediate impacts is through an operational-level grievance mechanism that is directly accessible to individuals, users and communities who may be adversely affected by the business and which can act as an early warning system about concerns. As with other dimensions of the corporate responsibility to respect human rights, the expectation that companies provide a remedy for harm they are involved in applies to all companies, foreign and Myanmar. Some of the larger Myanmar based companies are just beginning to address the need for establishing grievance mechanisms for workers, communities and civil society*[2] *as are some of the international companies operating in Myanmar.*[3]

Key Points for Implementation

- **Set up an accessible and local information point** for all issues concerning larger projects, and in particular network infrastructure. This could start with actions as simple as putting contact phone numbers on infrastructure if local villagers want to raise concerns about the equipment; it could also be a network of locally based liaison officers, or community volunteers, or a dedicated CSO with a two-way connection to the company.
- **For ISPs and "Over the Tops**": **Develop community standards** about the kind of content permitted on the site and mechanisms for users to report content they find disturbing (such as a "Report Concerns" button or link on the website). Undertake basic user awareness raising campaigns to ensure such mechanisms are known and effective.
- **Develop a mechanism (or mechanisms) that provides accessible and effective processes for users, workers or communities to address concerns directly** about a company or its business partners. Accessibility will need to be considered carefully in light of the services the company offers, local languages, availability of ICTs, or whether "toll free" services are available to call so that users do not have to pay.
- **Design any mechanism with worker and community input to be consistent with the effectiveness criteria** under the UN Guiding Principles on Business and Human Rights.[4] It should guarantee that there will be no retaliation against complainants inside and outside the company, and that complainants are free to choose whether to use the company's mechanism or opt for remediation processes by state or third-party institutions.

5. Take collective action where appropriate to address human rights, social and environmental issues.

There is a value to companies in the ICT sector coming together to approach sensitive topics collectively and sharing lessons learned on applying international standards, including from other comparable countries. Collective action by companies can be more effective, less labour intensive for Government, and reduce exposure for individual

[2] MCRB's, Pwint Thit Sa/Transparency in Myanmar Enterprises surveys companies for whether they have operational grievance mechanisms. On 3 June 2015 MCRB held Workshop for Business on Operational Grievance Mechanisms.

[3] See for example, Phillips reports that it has developed a Myanmar specific grievance mechanism: http://business-humanrights.org/en/response-by-philips-myanmar-foreign-investment-tracking-project

[4] UN Guiding Principles on Business and Human Rights, Principle 31 (see Recommendation to Government No. 9).

companies. There are a number of areas where companies may find it relevant to act collectively in discussions with the Government and other stakeholders.

Key Points for Implementation

- Collectively engage with the Myanmar Government **on filling the gaps within ICT and cross-cutting laws** to ensure alignment with international standards (See Government Recommendations 2 and 3).
- Collectively approach the Government on **applying international human rights standards around peaceful protest**, which are increasingly taking place using ICTs.
- Promote **learning on human rights issues** between foreign and Myanmar companies through engagement and support the creation of a sector-wide ICT industry association that includes foreign and domestic companies to support a coherent and coordinated approach to collective engagement.
- Work with development partners to **adapt higher education and vocational training** programmes to build skills for the ICT sector, and programmes to support SMEs.
- Support the variety of efforts across the country to **promote peaceful freedom of expression**, to counter hate speech, and to eliminate hate speech on ICT's.

6. Develop strategies for creating positive impacts at the local, regional and national level.

Key Points for Implementation

- **Develop social investment programmes with, for and by communities and users** to ensure focused, "strategic CSR" and ensure engagement and transparency around such programmes, including an annual public report and budget.
- **Promote small business and entrepreneurship programmes** to improve the ability of local businesses to meet ICT operator and subcontractor needs.
- **Commit to providing ICTs that are accessible to the disabled** and **improve livelihoods for people living with disabilities** in the country, given the very low level of employment for people living with disabilities or even access to services.
- Work with the government and other stakeholders to **provide access to language localisation and conversion resources.**

Recommendations
To CSOs, Human Rights Defenders and Media

1. Actively advocate for and comment on changes to ICT policy, laws and regulations, particularly with regard to human rights impacts.

Myanmar is in the process of developing or revising significant parts of the policy framework (such as the Master Plans cited in Recommendation 1 to the Myanmar Government), the laws and important regulations (such as under the 2013 Telecommunications Act, see Recommendations to the Myanmar Government, numbers 2 and 3). The Government staff and consultants working on these areas will be technical experts but potentially unfamiliar with the impacts on human rights of their policy advice. The same is true of Parliamentarians considering draft legislation.

Active civil society participation in advocating for and commenting on such changes will be important in ensuring that the final policy, legal and regulatory structure is appropriately balanced to provide for an efficient and effective ICT sector that guarantees protection of data and privacy and contains appropriate human rights safeguards. This should not only engage the limited number of Myanmar CSOs with ICT expertise; CSOs representing other interest groups such as women, ethnic minorities, children and people with disabilities should ensure their views are represented in ICT policy and legislation, since all are actual or potential users of ICT.

2. Hold companies to account on responsible business conduct, including around human rights.

There is an active, global discussion worldwide on the responsibility to respect human rights by companies in the ICT sector.[5] *Some of these discussions focus on company conduct and others focus on the increasingly complex interplay between companies and governments, in terms of the appropriate limits to government power to request or directly access private data held by companies. Some of the initiatives in the area are multi-stakeholder, with companies and civil society and sometimes also with government working on solutions together. Many of these resources have been cited throughout this SWIA (see the boxes on International Standards and Guidance, as well as Myanmar initiatives, at the end of each of Chapter 4 and Chapter 5). They provide guidance on what can be expected of companies in the ICT value chain that can be used by CSOs to engage in informed discussions with companies operating in Myanmar.*

[5] See for example the Business and Human Rights Resources Centre website on information technology and developments concerning companies in the sector.

3. Encourage companies and government to engage in multi-stakeholder discussion on human rights, social and environmental issues within the ICT sector.

There are no existing multi-stakeholder initiatives in Myanmar that will bring together companies, government and civil society into a common framework for discussion on ICT issues. The ICT Sector Working Group[6] *involves only government and international donors. The US Embassy has initiated the US ICT Council for Myanmar with support from the Myanmar Computer Federation. Under the Open Government Partnership, the government must consult civil society on its action plan. However OGP does not cover all the issues relevant to building appropriate safeguards into the ICT sector. At this stage, there are still opportunities to shape the long-term direction of the sector, learning lessons from elsewhere. Developing a multi-stakeholder discussion on the ICT sector could help further focus the Government's commitment to implement a people-centred approach, in line with growing international developments on a balanced approach to Internet governance.*[7] *The Myanmar Centre for Responsible Business (MCRB) stands ready to support such dialogues.*

4. Initiate and support efforts to educate the Myanmar public about safe and peaceful behaviour online, including counter-speech.

There is a clear role for civil society in helping to educate users on the dangers and opportunities of accessing ICTs in Myanmar. Given the wide range of languages in the country, it would be particularly useful for civil society organisations to make available information in Burmese and other languages, including clear and accessible explanations, training, awareness raising campaigns, etc. There is also a clear role for civil society in responding to and countering "hate speech", and providing concrete examples where online communities can support efforts around peaceful expression.

5. Increase media reporting on ICT sector.

Given the importance of the ICT sector to Myanmar, media outlets should increase informed reporting on the sector and its impacts to improve transparency, company and Government accountability, and public understanding. This should include reporting on complex and hidden areas such as the Government's lawful interception policies and practices.

[6] See "Sector working groups dashboard".
[7] See for example the Global Commission on Internet Governance.

Recommendations

To Development Partners & Home Governments

1. Support the strengthening of human rights, social and environmental considerations within ICT policy, legal and regulatory improvements, especially those highlighted in Recommendations 2 and 3 to the Myanmar Government.

Key Points for Implementation

- **Support the Myanmar Government to introduce of an effective framework for the ICT sector that includes adequate safeguards.** A number of partners including the Asian Development Bank (ADB), the World Bank, and the European Union (EU) are working on parts of the ICT regulatory framework. Given the past history of the country, it will be important to support the Government through both appropriate technical advice and political messaging, to ensure that the regulatory frameworks being put in place appropriately safeguard human rights. Any revised frameworks being supported with donor funding should not facilitate a return to excessive surveillance and repression. This might occur, for example, if the regulatory framework has been too broadly worded and allows wide latitude in interpreting and implementing the law. Development partners should ensure that the consultants hired by them or through the international financial institutions can and do provide appropriate advice, not only on technical matters but also on the balance to be struck in regulatory frameworks to ensure human rights are safeguarded.
- **Monitor whether the Government has developed its regulations on lawful interception** in line with international standards and good practice as set out in the Annex to the Recommendations.
- **Support rule of law changes to develop on-going checks and balances in the system** necessary to ensure implementation of an adequate ICT regulatory framework with appropriate safeguards. For example, the Government has indicated that it will require judicial review of lawful interception requests made by the Government. That is an important step, but it will be important to ensure that judges receive appropriate training and are part of a broader programme to strengthen the rule of law in Myanmar.
- **Support programmes to develop civil society capacity** to engage effectively with the Government on the extensive ICT reforms and with ICT companies (see Recommendations to CSOs, Human Rights Defenders & the Media above).
- **Support programmes to develop media capacity to report on ICT issues.**
- **Encourage the international financial institutions (IFIs)** working on ICT sector reform in Myanmar to make information and expertise available in order to engage a wider portion of Myanmar civil society and the population on the work they are doing.

2. Support implementation of the corporate responsibility to respect human rights by Myanmar and international companies.

> **UN Guiding Principles on Business and Human Rights: The State Duty to Protect**
>
> *2. States should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations.*

Key Points for Implementation

- **Home country governments should proactively express their expectations of companies domiciled in their country that are investing, or are looking to invest, in Myanmar.** This should include clear expectations that they should operate in line with the UN Guiding Principles on Business and Human Rights and, where relevant, the OECD Guidelines on Multinational Enterprises, including the requirements on disclosure. They should encourage companies to apply the IFC Performance Standards and WBG Environmental, Health and Safety Guidelines in the absence of Myanmar laws that provide for a higher standard.
- **Consider adopting reporting requirements modelled on the US Reporting Requirements on Responsible Investment in Burma**, or other reporting requirements for companies on environmental, social and human rights impacts (such as in the EU), and encourage companies to report specifically on Myanmar as a high-risk country for human rights.
- **Support the Government of Myanmar** in **introducing standards for responsible business conduct** for companies operating in Myanmar (See Recommendations to the Myanmar Government above).

3. Ensure investment and free trade agreements negotiated with the Government of Myanmar reinforce responsible business practices.

> **UN Guiding Principles on Business and Human Rights: Ensuring Policy Coherence**
>
> *9. States should maintain adequate domestic policy space to meet their human rights obligations when pursuing business-related policy objectives with other States or business enterprises, for instance through investment treaties or contracts.*

Key Points for Implementation

- **Ensure that investment, free trade, and other international economic agreements are coherent** with each country's or inter-governmental organisations' (in the case of the European Union) international obligations, including its international human rights treaty obligations, and make reference to the UN Guiding Principles on Business and Human Rights.
- **Ensure that each party to such agreements has preserved sufficient "policy space"** (freedom to make policy changes and choices after the agreement is formalised) for further changes to domestic policy that can improve environment, social and human rights protections. Governments should ensure that those agreements reinforce rather than restrict good governance and responsible business practices.

Recommendations
To Investors

1. Conduct due diligence on companies in portfolios that are involved in the ICT sector in Myanmar.

This should include enhanced due diligence regarding their policies, systems, reporting and responses to specific human rights challenges in Myanmar. Investors should understand if the companies they invest in are creating risks to human rights and if so, the steps the companies are taking to prevent and mitigate those risks and remedy impacts.

2. Engage with investee companies involved in the ICT sector in Myanmar to ensure that these companies meet international standards on responsible business conduct relevant to their business in Myanmar.

This might involve direct engagement or participation in shareholder actions.

3. Urge companies doing business in the ICT sector in Myanmar to report robustly on how they manage risks and impacts associated with investments and operations in the country.

The US Government's Reporting Requirements on Responsible Investment in Burma could be used as a framework for such disclosures.

Recommendations
To Users

1. Undertake basic steps to protect your privacy and security while using ICTs.

- **When using social media:**
  - **Avoid publicly** sharing personal information such as bank statements, address, email address, date of birth or mobile phone numbers on social media or mobile applications.
  - Use privacy **settings** to control what other users can see or access on your profile.
- **When using online services:**
  - Use **strong passwords**, which: [8]
    - Are at least eight characters long
    - Do not contain your user name, real name, organisation name, or a complete word
    - Are significantly different from previous passwords
    - Contain uppercase letters, lowercase letters, symbols and numbers
  - **Avoid using the same password for different services, e.g. Facebook and Gmail**.
  - Keep these passwords **safe and confidential**.
- **When using email:**
  - **Avoid** opening emails with **file attachments from unknown senders**.
  - Use a **different email address** for online services than the email address used for personal email communication.
- **When browsing the Internet:**
  - Use **"private browsing" settings** in Chrome, Firefox, Safari, or Internet Explorer. Private browsing prevents websites from remembering your login information and prevents your browser from logging websites you visit under your browsing history.

[8] Microsoft, "Tips for Creating a Strong Password" also see Micah Lee, The Intercept, Passwords you can Memorize- But That Even The NSA Can't Guess (26 March 2015) for additional guidance on designing strong passwords.

Annex to the Recommendations

Lawful Interception and Government Access to User Data: The Characteristics of a Rights-Respecting Model

Purpose

At the time of this report, a key part of Myanmar's telecommunications framework on lawful interception (LI) had yet to be finalised. Regulators need to define the limits of lawful communications surveillance and clarify the capabilities and the uses of communications surveillance technology used for lawful interception, which refers to access of communications content in real time. The section below lays out the characteristics of a framework that protects human rights to cover both lawful interception and government access to user data. Both are considered to be acts of surveillance.

The distinction between lawful interception and access to user data is that lawful interception covers real time access to communications and access to user data is about historical data, known as "communications data".[9] In many countries the laws governing what can be accessed, and when, make distinctions between the two, with a higher burden of proof to authorise lawful interception.

In recent decades, both physical and communications surveillance was widely conducted in the absence of a legal framework or oversight. There is an opportunity for the Government of Myanmar to develop legal protections that respect human rights, as part of the wider 'people-centred' reforms, and to take a leadership position within the region. Such a lawful interception framework will build trust in the use of Myanmar's ICTs among users, service providers and other governments by being robust and aligned with international human rights standards.[10]

As outlined above, the only existing legal framework is Article 75 of the 2013 Telecommunications Law, which allows interception but does not clearly articulate definitions or justifications.[11] The Government of Myanmar has asked the European Union for technical assistance in drafting implementing legislation. To assist this drafting

[9] Communications Data (sometimes referred to as metadata) is basically everything but the content and includes telephone numbers of both the caller and the recipient, the time and duration of a call, unique identifying numbers (each subscriber is allocated one, as is each mobile device), email addresses, web domains visited and location data. This information is important as it builds up a detailed picture of a person's life and movements, so that often intercepting the content of a call or email is not necessary. In contrast to content, there are often weaker legal protections around interception of stored communications data.

[10] See for example: See for example the Global Conference on Cyberspace 2015, the Global Commission on Internet Governance

[11] Article 75 states: "*The Union Government may, as may be necessary, direct to the relevant organization for enabling to obtain any information and telecommunications which causes harm to national security and prevalence of law without affecting the fundamental rights of the citizens.*" See unofficial English translation of the Telecommunications Law (2013)

process, MCRB has conducted preliminary research into what the characteristics of a human rights respecting model of lawful interception might look like in Myanmar. These findings are presented below and aim to provide useful information to the Government of Myanmar and other stakeholders involved in drafting this legislation, including the 2016 Parliament.

These recommendations[12] set out the principle considerations as the Government of Myanmar begins to develop an approach to regulation and legislation on communications surveillance covering 7 main issues:[13]

The Characteristics of a Rights-Respecting Lawful Interception Model

1. Prerequisites
2. Authorisation Processes
3. Oversight
4. The notification of individuals
5. Remedy
6. Transparency
7. Provision for Framework Review

1. Prerequisites Before Lawful Interception Should be Considered

- Lawful interception should be undertaken only when other potential measures that could have been used to deal with the criminal or national security threats have been exhausted, for example other police measures that do not involve surveillance.
- Any type of surveillance should be carried out only on targeted suspected individuals and organisations where there is prior suspicion that the targeted subject is suspected of a crime.[14]
- Misuse of intrusive capabilities should be a criminal offence and surveillance used outside the legal frameworks should be prohibited.
- The legal framework authorising lawful interception and access to user data should be established through primary legislation and debated in the legislative branch, rather than being adopted as subsidiary regulations enacted by the executive. Public consultation and involvement of stakeholders is a vital part of the policy-making process because many of the processes under the legislation will be carried out behind closed doors, without the opportunity for public scrutiny. It is even more important therefore that the public has a say in establishing the framework.
    - The Government of Myanmar has committed to a public consultation of draft lawful interception regulations.[15]

[12] These recommendations draw on recent reports to the UN General Assembly and Human Rights Council, including the Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/23/40 (June 2013); The Right To Privacy in the Digital Age, UN Resolution 68/167 adopted 21st January 2014 ; Report of the Office of the United Nations High Commissioner for Human Rights, presented to the Human Rights Council in September 2014 A/HRC/27/37 and the Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism to the UN General Assembly in September 2014 A/69/397

[13] The issues addressed cover both lawful interception (real time access to communications) and access to historical data (which has a number of different terms in law in different jurisdictions including communications data and metadata,

[14] See: UN General Assembly A/69/397 23rd September 2014

[15] See the announcement on p5 of the Public Consultation Issued by the Ministry of Communications and Information Technology of the Republic of the Union of Myanmar. Proposed Rules for Telecommunications

2. Authorisation Processes

- Specific instances of communications surveillance should be authorised by an **independent** and **competent** judicial authority prior to surveillance taking place. Some states have a process of executive sign-off rather than judicial authorisation.
- **Independence** in this circumstance means separate and not connected to the authorities that will be carrying out the surveillance. **Competence** means that those with responsibility for giving authorisation must have sufficient knowledge of the issues, both technologically and from a human rights perspective. This independence and competence is absolutely critical to the integrity of any legal framework. Some states have a process of executive sign-off rather than judicial authorisation. But the prevailing view at the UN level and among civil society is that judicial authorisation is preferable for its independence (the Authorising Authority).
  - The Government of Myanmar has already committed to judicial authorisation.[16]
- Communications surveillance must be limited to that necessary to achieve a legitimate aim and use the means least likely to infringe rights; it must be both necessary and proportionate. An objective assessment of the necessity and proportionality of the contemplated surveillance should be a core part of the authorisation process.
- The legal framework should set out which agencies among government bodies can request lawful interception (the Requesting Agencies).
- The legal framework should also set out the criteria and conditions on which the court will make the decision on whether to authorise the request.
- Any authorisation should be time-bound with a requirement for the Requesting Agency to return to the Authorising Authority to request a renewal as that period of time expires; automatic renewals of surveillance requests should not be permitted.
- The legal framework should set out clear limits on the amount of time that data collected can be stored. It should require that data is destroyed once the period expires. In addition, it should require that any data illegally collected is immediately destroyed and not used.

3. Oversight

- There is an on-going global debate about the best form of oversight of lawful interception and access to user data. Increasingly there is interest in mixed models of oversight that incorporate administrative, judicial and parliamentary actors.
- Oversight must be vested in another body (or bodies) that is independent of the Authorising Authority that originally authorised the surveillance.
- Oversight must be rigorous and not a rubber stamping exercise.
- Consideration should be given to permitting a confidential public interest advocate, for example an independent human rights expert, within the surveillance authorisation process to ensure that appropriate consideration is given to the human rights implications of the request. This is particularly important given the high degree of secrecy of authorisation processes that relate to national security.
- The oversight body must have access to all potentially relevant information to enable it to evaluate whether the government is carrying out its activities in a lawful way. This must include secret and classified information. Third parties, for example companies, should have the ability to bring relevant information to the oversight body.
- The oversight body must have the resources and expertise to be able to carry out effective oversight.

Sector Relating to Licensing, Access and Interconnection, Spectrum, Numbering, and Competition (November 4, 2013)

[16] Telenor Myanmar sustainability presentation (August 19th 2014). See p8 of the transcript.

- Within the oversight regime there must be regular reporting to the public on whether the government is carrying out its surveillance activities appropriately, in a way that helps the public understand whether the government has followed the procedures.
- Oversight will usually happen at a defined time after surveillance has taken place (often with a regular report to the Parliament or public) and is designed to test whether surveillance that has already happened took place in accordance with the framework the country has in place.

4. Notification of Individuals under Surveillance

- It is understood that there will be times when individuals cannot be notified that they are under surveillance as to do this could jeopardise the surveillance itself.
- However, notification of individuals if they have been the subject of surveillance is an important part of the framework in a country to give individuals who may have been subject to illegal surveillance access to remedy**.** At a minimum, users should be notified that their communications have been subject to surveillance when the surveillance is complete.
- The legal framework should set out the circumstances under which there may be a delay in individuals being notified that they are under surveillance and the authorising body for this.

5. Remedy

- Individuals need to know whether they have been the subject of surveillance in order to bring a complaint and obtain a remedy for surveillance that was carried out not in accordance with the law. When individuals are informed that they have been the subject of surveillance they should also be informed of the procedure for filing a complaint if they wish to do so,
- Any alleged violation must be promptly, thoroughly and impartially investigated.
- Where a violation is identified it must be possible to end it. For example, the body examining the potential abuse must be able to order the termination of the surveillance and the deletion of data and prohibition of its use by issuing binding orders.

6. Transparency

- The legal framework concerning communications surveillance must be publicly accessible and set out the nature, scope and time-frame of possible surveillance, the requirements that must be met for surveillance to be authorised, and which authorities are responsible for authorisation, carrying out and supervising the surveillance. The process for remedy for individuals who have been the subject of inappropriate surveillance must be explained, as should the circumstances in which there can be sharing of information across borders between governments. There should be a clear explanation of each different type of surveillance that is possible. See below for some of the current issues that are being addressed in international and national debates relating to this.
- The publicly accessible information about surveillance set out in the law must be sufficiently clear and precise for individuals to be able to understand it and foresee how the law might be applied to them.
- To promote government accountability, the government should produce, as a minimum, the aggregate yearly figures on the specific number of requests for surveillance it has made, including the number accepted and rejected, details of the way in which it has been using its powers, and information broken down by specific legal authority for example, wiretaps, the number of requests to service providers, etc.

7. Provision for Periodic Review of the Lawful Interception Framework

- Given the speed at which technology develops, and the potential for communications surveillance to infringe rights, it is important that there is provision within the legislative or regulatory framework for periodic review of the law to ensure rights are protected.

Other Considerations to Take into Account in Drafting the Legal Framework

- **Consistency between the regulation, law and practice:**
  - Embedding human rights principles into the regulation and laws that provide the framework for interception and surveillance is insufficient on its own.
  - The agencies requesting surveillance must be required to consider the human rights implications in the requests that they make. This should include consideration of whether any less intrusive methods are possible, to ensure that the issue of proportionality is addressed.
  - There should be training on the human rights implications and their obligations to consider them for all agencies who have the powers to make requests. Training the judiciary is also required.
  - Accompanying the legal framework there should be a more detailed code of practice that sets out how the law is intended to work in practice.
  - Where there is more than one law or regulation in place (e.g. telecoms law, national security law, tax, drug enforcement, cybersecurity legislation etc.) there must be consistency in the human rights safeguards in place and clarity provided on which law has primacy in which circumstances.

- **The role of companies providing service to users:**
  - Service providers should not be compelled to modify their infrastructure to enable direct surveillance that eliminates the opportunity for judicial oversight.
  - Any request to service providers for access to communications content or data should be provided in writing, explaining the legal basis for the request including the requesting government entity and the name, title and signature of the authorised official. Although it is preferred for requests to be provided in writing it is recognised that there are certain exceptions provided for by law, for example emergency situations and immediate risk to life where oral requests are acceptable, providing they are followed up in writing.
  - Service providers should have the right to seek clarification or modification to a request which does not seem to follow domestic legal procedures (which in turn should incorporate the internationally accepted human rights protections).

- **Areas of Current International and National Debate on Lawful Interception:**
  - Many countries require a higher degree of authorisation for access to communications content than they do to access communications data or metadata. Metadata / communications data can give more insight into a person’s life than was historically the case with simple telephone call and duration information, for example, mobile location data. This has resulted in an active debate about whether this lower level of protection that is given to communications data or metadata is still appropriate. Some countries have recommended the consideration of a third category of data, in addition to communications content and metadata/communications data. This proposed third category would give greater protection to certain types of communications data considered more sensitive, such as websites visited and a user's location from a smartphone.
  - The leaks from Edward Snowden regarding the surveillance activities of the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) have put the spotlight on “mass surveillance.” There is no international agreement on what this term means in different jurisdictions. At the UN level there is serious concern about communications surveillance authorised on such a broad and indiscriminate basis. This runs counter to the core concept of the protection of privacy that requires justification to be made on a case-by-case basis.
  - The issue of whether nationals of a particular country should enjoy higher protection than non-nationals is a current debate. The International Covenant on Civil and Political Rights (ICCPR) by its terms provides protection to all, without distinction based on nationality.
  - Laws that authorise extra-territorial surveillance or the interception of communications in foreign jurisdictions are problematic, for example because of an individual’s inability to know if they are subject to surveillance and therefore potentially seek redress.