Myanmar Centre for Responsible Business

18 March 2022

Myanmar Centre for Responsible Business (MCRB) welcomes the opportunity to submit experience from Myanmar in response to the call for input to the High Commissioner report on the practical application of the UNGPs in the tech sector. Our input specifically addresses '**The State's duty to protect, or regulatory and policy responses'** (session four). It summarises MCRB's research and advocacy in this area over the last eight years in Myanmar, and lessons learned. It also includes suggestions lessons for member states in their role in promoting respect for human rights by technology companies, including through their development programmes.

MCRB's Sector-Wide Impact Assessment (SWIA)

In association with its co-founder, the Institute for Human Rights and Business (IHRB), MCRB embarked upon a Sector-Wide Impact Assessment (SWIA) of Myanmar's ICT Sector in 2014. At the time the sector was expanding rapidly. Drawing on the methodology developed for MCRB's first two SWIAs on oil and gas, and tourism, in which the UN Guiding Principles were central to the approach, the assessment analysed Myanmar's ICT policy and regulatory framework from the perspective of whether it protected human rights. It also undertook research on the ground, based on interviews with a variety of stakeholders and rightsholders including companies, users, and regulators.

Both 'offline' and 'online' rights were assessed. The former related primarily to network infrastructure rollout. The latter covered issues relating to Freedom of Expression, 'Hate Speech', Privacy, Surveillance and Lawful Interception and Cyber-Security.

Of the stakeholders interviewed for the SWIA, it was the companies (or at least a minority of them, particularly Telenor and Ericsson) which were most aware of the risks to human rights in the regulatory framework, above all those concerning surveillance/lawful interception. They had identified these in their human rights due diligence undertaken prior to market entry.

The ICT sector is one of the few areas of legislation in which companies who seek to respect human rights can be prevented from doing so by legislation or local context. Generally other legislation, for example labour, sets a minimum standard, on which companies have the freedom to improve to ensure human rights are respected. Consequently, companies that seek to respect human rights have an active interest in identifying and reforming regulations which do not contain human rights safeguards. The Global Network Initiative (GNI) is one manifestation of that.

At the time, the main law applicable to the sector was the newly adopted 2013 Telecommunications Law (which was not finalised when companies were first bidding for telecom licences). There were also some legacy laws which created risks to human rights identified in the SWIA. Generally, the protection of human rights was not recognised in any ICT-related laws. The Telecoms Law contained broad provisions without safeguards on several issues including internet shutdown and lawful interception (surveillance), as well as defamation (a topic covered in multiple Myanmar laws). Further details on the regulatory framework and human rights risks are available in Chapter 2 of the SWIA, and summarised in Table 11, Chapter 2) (see also the GNI's Country Legal Framework Resource database for Myanmar).

The ICT SWIA was published in October 2015 after a consultation on the draft report and recommendations. In addition to the assessment of human rights risks and impacts, the SWIA includes recommendations to all stakeholders, including government. To the Myanmar government, these were:

1. Establish a coherent policy framework for the ICT sector with adequate safeguards.
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.
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.
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" (detailed recommendations were provided for a rights-respecting model)
5. Improve data protection standards and cybersecurity.
6. Demonstrate a commitment to free and open communication through a modern Freedom of Information law and build meaningful transparency systems across Government.
7. Accelerate the implementation of Myanmar's universal service commitments.
8. Improve digital literacy of users and send clear signals about respectful use of ICT's.
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.

Each of recommendation was aligned to specific UNGPs, and came with detailed pointers for implementation.

MCRB's 2015 SWIA was prescient in predicting human rights risks associated with the legal framework and lack of human rights safeguards. These have since materialised as a result of exercise of the legal provisions by the authorities. They include the first use of internet shutdowns in Myanmar in June 2019 in townships in Rakhine and Chin State as well as government requirements for surveillance which they sought to enforce the following year. An increasing number of individuals, including government officials and politicians, but also private citizens, used the defamation clause '66d' concerning criticism on social media, and this increased after 2016. It is notable that these human rights risks materialised under the elected National League for Democracy government. Shutdowns have intensified following the 1 February 2021 military coup, with internet shutdowns and website blocks widespread.

Follow up Advocacy on Policy and Regulation

Following publication of the SWIA in October 2015, MCRB pursued advocacy with government, Parliamentarians, and the National Human Rights Commission in line with the SWIA recommendations.

SWIA Recommendations and updates were distilled into policy briefs in early 2019 on:

- The Legal and Policy Framework for Information Communication Technology (ICT) In Myanmar: Implications for Human Rights
- Cyber Security and Cyber Crime: Issues for Myanmar
- A Data Protection Law That Protects Privacy: Issues for Myanmar

Advocacy was sometimes undertaken jointly with the growing number of civil society organisations (CSOs) with an interest in digital rights and/or companies, particularly members of the Global Network Initiative. GNI member companies were keen to work collectively with MCRB to pursue rights-protecting regulatory reform as they recognised that the legal framework could prevent them from meeting their responsibility to respect human rights. This concern became a reality for Telenor and contributed to its decision in July 2021 to exit Myanmar. An explicit requirement to install interception equipment was placed on all mobile operators prior to the 1 February 2021 coup. Following the coup, heightened human rights risks associated with assisting surveillance amidst 2018 EU and Norwegian sanctions on surveillance equipment led Telenor to exit Myanmar.

MCRB made written submissions to consultations. based on the UNGPs, on draft secondary legislation on issues such as mandatory SIM Card registration, and internet gateway services guidelines, with comments focussed on the privacy/data retention aspects of the proposal. MCRB also submitted comments on the 2015 draft Telecommunications master plan covering issues such as transparency, universal access and service, data privacy and responsible business conduct, having successfully encouraged the Ministry to undertake an open consultation process. It should be noted that the Ministry of Telecommunications (later Transport and Communications), perhaps due to support on Telecoms Sector Reform from the World Bank, was generally more systematic in seeking comments on draft regulation and policy than other Ministries. The main responders to consultation were the business community, not least due to the lack of civil society focus on, or understanding of, the sector until recently. MCRB sought to encourage the widest possible input whenever a consultation was announced.

MCRB and other organisations also conducted written and in-person advocacy, towards the Parliament in September and October 2016, which had drafted (without regulator input) a Citizen's Privacy and Security Protection Law. Advocacy was focussed primarily on the need for safeguards on lawful interception. This was treated as little more than one line in the law, and therefore failed to provide the necessary safeguards and oversight. During the 2016-2020 period, MCRB also sought, with others, to engage on the draft 'hate speech' law although the opaque policy and regulatory process made this challenging.

MCRB participated in consultations in Naypyidaw in January 2019 on a draft cybersecurity framework, combining this with a briefing for relevant parliamentary committees on digital rights issues, and legislation and policy gaps. (The evolution of this regulatory framework is charted on MCRB's website, including the latest consultation draft circulated in January 2022).

In all this advocacy, the three-pillar framework of the UNGPs was always used to help stakeholders understand the respective roles and responsibilities of government and business, since regulators and legislators were often unfamiliar with business and human rights.

Multistakeholder approach to policy and regulation – Myanmar Digital Rights Forum

To build awareness of digital rights issues (mainly freedom of expression, privacy and access/inclusion) and to promote multistakeholder dialogue, MCRB was one of the instigators and co-hosts of the Myanmar Digital Rights Forum. This was first held in December 2016 and again in 2018, 2019 and February 2020, with support from the Swedish government. Several hundred participants attended, mainly from business and civil society, as well as international experts and development partners. Although there was some participation from government officials who were given speaking roles, there was very little participation from MPs. Indeed, finding MPs who were interested in digital rights remained challenging.

Generally the conclusions of the Forum highlighted the need for digital policy and regulation that protects human rights. MCRB and MDRF co-organisers sought to bring this to the attention of regulators and legislators following the Forums.

The role of development partners

Throughout this period, MCRB sought to engage development partners in the digital rights agenda, via their diplomatic missions represented in Myanmar. The SWIA contained recommendations to development partners/home governments to

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.
2. Support implementation of the corporate responsibility to respect human rights by Myanmar and international companies.
3. Ensure investment and free trade agreements negotiated with the Government of Myanmar reinforce responsible business practices.

However, it proved quite difficult to engage the diplomatic community and development partners on digital rights issues. The exception was the World Bank, who were generally open to ensuring that the 2014 technical assistance on telecoms sector reform took human rights into account, although this was not programmed in up front.

This may reflect – at least at the time - a general lack of consideration of digital rights in the frameworks for ESG risk screening of projects by development finance institutions, even though they are increasingly making ICT investments. For example neither CDC's ESG Toolkit, whose sectoral guidance on telecommunications nor the IFC's EHS guidelines for the Telecommunications sector make any mention of risks to digital rights, and only cover offline risks. When these digital rights risks such as surveillance and shutdown started to materialise in Myanmar, impacting on their investee companies, some DFI investments had to rapidly consider risk management options.

Lawful Interception – a missed opportunity to support better regulation

From an early stage, MCRB and telecoms companies encouraged others, particularly the EU, to provide support to the Myanmar government to fill the gap and create a rights-respecting regulatory framework for lawful interception. Although telecoms companies were some of the best placed to identify effective rights-respecting LI frameworks (and the Global Network Initiative's Country Legal Frameworks Resource is a useful compendium of national legal practices), companies believed that it would be inappropriate for the private sector to take a lead role in supporting the Myanmar government to draft laws, and that this was a role for development partners.

In early 2015, at the encouragement of MCRB and companies, the Myanmar authorities made a request to the EU Delegation in Myanmar to help draft a law for the interception of communications. In response, the EU chose to piggyback on an existing EU funded Council of Europe project on Global Action on Cybercrime (GLACY). Experts from this project provided the Myanmar government in 2015 not the draft LI legislation that they had requested, but a document of **'Generic legislative language on cybercrime and electronic evidence'**. This document was based on the provisions of the 2001 Budapest Convention on cybercrime, which was already over a decade old. Furthermore, Article 15 of the Budapest Convention (Conditions and safeguards) which contains language on human rights protections was not included in the document given to the Myanmar telecoms regulator (PTD) who after consideration, concluded that it was not relevant to their request, and passed it to the (military-controlled) Home Ministry. They took no action until passing it back to the Ministry of Telecommunications several years later. A major opportunity to

support a 2015 request from the government of Myanmar to fulfil their duty to protect human rights when undertaking lawful interception/surveillance was therefore lost.

Furthermore, although MCRB encouraged the EU Special Representative to include digital rights as part of the EU/Myanmar human rights dialogue, as it had the potential to be a genuinely two-way dialogue around dilemmas that could bring in officials from across government, this was never included in the agenda.

Making more use of the Freedom Online Coalition

This incident was indicative of a wider challenge relating to development partners/diplomatic missions in Myanmar. There was low awareness of the human rights issues associated with technology, and of the diplomatic and development importance of the topic (although press coverage and increased awareness in recent years around the rights risks posed by social media etc have begun to change this). The **Freedom Online Coalition (FOC)**, a group of 34 countries committed to protecting and promoting online freedoms domestically and abroad, was established in 2011 to promote diplomatic coordination by governments on these topics. FOC Members have agreed to prioritize three primary activity areas:

1. Strengthening coordination and cooperation among Members, as well as with outside stakeholders who share the Coalition's objectives, with added focus on fostering cross-regional diplomacy through employing local networks;

2. Shaping global norms on human rights online through joint statements;

3. Holding periodic convenings with Members and other stakeholders.

However, to date the FOC appears to be mainly a headquarters initiative without connection to opportunities on the ground to progress its agenda. In Myanmar, Embassies of governments who are FOC members lacked awareness of the FOC. This was true even for the in-country missions of the country holding the Chair of the FOC, who appeared unbriefed by headquarters. The FOC Chair (Canada in 2022) is supported by Friends of the Chair (Denmark, Estonia, Finland, France, Germany, Ghana, the Netherlands, Switzerland, the United Kingdom, and the United States), many of whom are active in Myanmar. With a total of 17 government members of the FOC having resident missions in Myanmar, the FOC could be a platform for more active in-country coordination and action among diplomatic missions on digital rights issues, including coordinated diplomatic and development action, together with UN institutions and IFIs.

For example, embassies in June 2019 with one notable exception (Sweden) were not proactive in speaking out on issues such as internet shutdown. Nor do donors coordinate and consult on issues related to the tech sector and human rights including its integration into other programmes such as health, education or democratisation and the rule of law.

Conclusions

Despite the SWIA's success in analysing and predicting human rights risks in the policy and regulatory framework which subsequently – and unfortunately - materialised, the six years of follow-up advocacy was less successful. Little progress was made in achieving regulatory and policy responses that are consistent with the State's duty to protect.

Consequently while the military government which took over on 1 February 2021 unilaterally rescinded some human rights protections in other parts of the legal framework, most of the digital rights safeguards for which MCRB and other civil society organisations had advocated for did not need to removed as they

were not there in the first place. Instead, the State Administration Council has been able to make use of a legal framework in the Telecommunications Law which is broadly unchanged since 2013. Additionally, draft laws on cybersecurity, which now includes a potential prohibition on VPNs, and another draft law on 'hate speech', both of which were under development during the NLD government, may be adopted by the military regime without parliamentary scrutiny. While it is encouraging however that both Myanmar and international businesses have collectively advocated for changes to the draft cybersecurity law, it is unlikely that the adopted versions of either law will incorporate the state duty to protect human rights.

There may be wider reasons that advocacy for a better policy and regulatory framework has not to date succeeded in Myanmar. There are global and regional trends towards countries adopting ICT laws which are increasingly illiberal (although the ASEAN Digital Masterplan 2025 has highlighted the need for better regulation to protect privacy and open internet as a priority).

However, at the Myanmar level, a major challenge was low digital literacy amongst Myanmar regulators and legislators. Technical assistance programmes tended not to include these basics. Many even lacked access to computers or email, and few if any could be considered 'digital natives' or even comfortable with technology. This meant they lacked confidence and/or interest in engaging on the ethical and human rights issues relating to ICT, and how to reflect these in policy/regulatory approaches.

Under the government of the National League for Democracy (2016-2020), the merger of the Telecoms Ministry with the Ministry of Transport and the appointment of septuagenarian Ministers from a transport background further reduced any political leadership on digital issues since in the 2011-2015 period. The Government lacked a digital champion that could drive policy and legal reform, including human rights protection.

Siloed government, and the absence of a ministry leading on human rights (e.g. a Ministry of Justice) meant that issues which needed a cross-government approach such as privacy, freedom of expression and data protection were either ignored or left with ICT technocrats, including Russian/China-trained ex-military Signals Branch, who had transferred to the Ministry.

The lack of activity on digital rights from embassies/development partners, as highlighted above, exacerbated these gaps. It meant that digital rights were rarely considered as part of the significant technical assistance provided between 2013 and 2021 to a variety of government departments.

While MCRB's experiences have been specific to working on human rights and the UNGPs in the tech sector in Myanmar in the last eight years, they may resonate with other country situations. It is hoped that this submission will be helpful in encouraging government to put more weight on digital literacy amongst government and institutional employees and elected officials, so as to support more effective government action to protect digital rights at national and international level.

Myanmar Centre for Responsible Business

www.mcrb.org.mm