In Myanmar's tumultuous landscape, the intersection of information and communication technologies (ICT) with government surveillance poses grave threats to freedom of expression and privacy. My talking points delve into the intricate web of challenges faced by civil society and businesses alike in upholding human rights amidst conflict.

Based on the comprehensive report by ETIF, we provide an overview of the state of surveillance in Myanmar. The report sheds light on how the government obtains personal information from ICT companies to commit human rights violations. The research was conducted by esteemed consultants Dr. Daniel Aguirre and Dr. Irene Pietropaoli, and it provides a thought-provoking analysis of the situation in the country.

1. Surveillance and Human Rights Violations: I will examine the alarming extent of surveillance practices in Myanmar and their direct correlation with human rights infringements.

2. Involvement of Private Sectors: Ill mention complicity of ICT companies in providing surveillance technology to the regime, implicating them in the erosion of fundamental freedoms.

3. **Myanmar Legal Framework**: Against the backdrop of a complex regulatory framework, we dissect the legal landscape in Myanmar, highlighting its inadequacies in safeguarding privacy and other human rights. Such as:

- *Telecommunications Law 2013 (amended in 2017):*[1] Several provisions of this law enable surveillance. Section 75 allows the government to require 'the relevant organisation' to provide access to information and telecommunications which cause harm to national security or respect for the law 'as may be necessary'. Although there is a clause calling for respect for fundamental rights, the vagueness of this provision and lack of concrete procedures could easily provide legal cover for problematic surveillance practices. Similar concerns are raised by section 76, which enables entry and inspection of telecommunications service providers for matters related to national defence, security, or the public interest.

  In emergencies, section 77 also empowers the Ministry of Transport and Communications to order suspensions of telecommunications services, intercept or obtain information, cease operations of specific forms of communication, or temporarily control telecommunications equipment. Emergencies are not clearly defined and the military has declared the country under a state of emergency since the 2021 coup.

- *Counter-Terrorism Act 2014 (amended in March 2023):* Section 47 empowers a counter-terrorism committee to issue orders for the interception or restriction of electronic

[1] *Telecommunications Law*, No. 31/2013, 8 October 2013, translation into English at: https://www.mlis.gov.mm/mLsView.do;jsessionid=873EF072104248EAB3CBDDB2DE19F143?lawordSn=1076; translation of 2017 amendment at: https://myanmar-law-library.org/topics/myanmar-telecoms-law/pyidaungsu-hluttaw-no-26-17-amendment-of-telecommunications-law.html. For a full analysis of this law see ARTICLE 19 (2017) 'Myanmar: Telecommunications Law, 2013', March, https://www.article19.org/data/files/medialibrary/38665/Myanmar-analysis--8-March-2017.pdf.

communications of 'terrorist groups and terrorists'.[2] New Counter-Terrorism Rules issued in 2023 set out procedures for this interception. These lack basic due process protections and the authorising committee is not independent from the military.[3] The Rules explicitly state that telecommunications companies shall not refuse the committee's orders to intercept or restrict communications.[4] These powers are likely to be applied extensively, as the military has applied the terrorist label broadly, including to members of the civil disobedience movement and peaceful opposition.

- *Law Protecting the Privacy and Security of Citizens (2017; amended 2020 and 2021)* (Privacy Law):[5] This law provides some very general privacy protections but does not constitute a proper data protection regime. Shortly after the 2021 coup, the military announced an amendment which suspended some sections of the Law for as long as the State Administration Council is governing the country.[6] The suspended privacy protections included prohibitions on intercepting communications or accessing personal data from telecommunications operators without a warrant or lawful permission.

- *The Electronic Transactions Law 2004 (amended in 2014 and 2021)* (ETL):[7] The military introduced amendments to the ETL requiring those managing personal data to protect such information and imposing criminal penalties on those who obtain, disclose, use, destroy, or disseminate personal data without consent. These obligations are only described briefly and in very vague terms, posing serious compliance challenges for the private sector.[8] They also contain broad exceptions for government authorities, such as to gather information about

---

[2] *Counter Terrorism Law*, No. 23/2014, 4 June 2014, translation into English at: https://www.mlis.gov.mm/mLsView.do;jsessionid=5B029BFB369BF0AA41D22495C5A69293?lawordSn=9596.

[3] Access Now (2023) 'Myanmar's "Counter-Terrorism" By-Laws Must Be Denounced for What They Are – Illegal', 19 April, https://www.accessnow.org/myanmar-counter-terrorism-law/. Partial translation of by-laws into English at: https://www.lincolnmyanmar.com/wp-content/uploads/2023/03/Counter-Terrorism-Rules-abbreviated.pdf.

[4] *Ministry of Home Affairs (Counter-Terrorism Rules)*, Notification No. 239/2023, 1 March 2023, Rule 80(d), as translated into English at: https://www.lincolnmyanmar.com/wp-content/uploads/2023/03/Counter-Terrorism-Rules-abbreviated.pdf.

[5] *Law Protecting the Privacy and Security of Citizens*, No. 5/2017, 8 March 2017, English translation (with post-coup military changes integrated) at: https://www.myanmar-responsiblebusiness.org/pdf/Law-Protecting-Privacy-and-Security-of-Citizens_en_unofficial.pdf.

[6] State Administrative Council Law No. 4/2021, 13 February 2021, English translation at: https://www.gnlm.com.mm/amendment-of-law-protecting-the-privacy-and-security-of-the-citizens.

[7] *Electronic Transactions Law*, State Peace and Development Council Law No. 5/2004, 30 April 2004, translation incorporating 2014 amendments and 2021 post-coup changes at: https://www.myanmar-responsiblebusiness.org/pdf/electronic-transactions-law_consolidated_2014-and-2021_en.pdf.

[8] Allen & Overy (2021) 'Update from on the ground: Changes to the Electronic Transactions Law and the impact on financial institutions operating in Myanmar', 15 March, 2, https://www.jdsupra.com/legalnews/myanmar-update-from-on-the-ground-2373099.

cybersecurity issues of concern to peace, stability, or national security, which offer a legal excuse for government access to personal data.

- *Draft Cybersecurity Law (2021; 2022):* Just days after the 2021 coup, the military circulated a draft Cybersecurity Law. However, after substantial backlash from the business community and civil society, it dropped the draft, although a few provisions were integrated into subsequent amendments to the ETL.[9] In 2022, a revised draft was again proposed.[10] It is unclear whether the military still intends to introduce this law, which raises serious freedom of expression and privacy concerns. The draft Law would impose registration requirements and other onerous obligations on digital service providers, create new intrusive regulatory powers over such providers, and impose local data storage requirements. It would also criminalise the use of VPNs without government permission.

4. Recommendations for CSO Engagement Strategy: Recognizing the critical role of civil society, we propose a strategic roadmap for Myanmar's CSOs to engage with responsible businesses. This includes advocating for policy reforms, fostering transparency, and holding corporations accountable for their actions.

Advocacy and Awareness Raising:

1. Engage with the international community
2. Work with the Freedom Online Coalition
3. Raise awareness about freedom of expression, privacy and data protection among Myanmar people
4. Secure Personal Data and Financial Transactions
5. Discuss risks related to human rights with Myanmar business
6. Use international standards and industry-led initiatives to engage with companies operating in Myanmar

---

[9] See description of developments at Myanmar Centre for Responsible Business (15 February 2022) 'Update on Draft Cybersecurity Law and its Impacts on Digital Rights and the Digital Economy', https://www.myanmar-responsiblebusiness.org/news/draft-cybersecurity-law.html. ARTICLE 19's statement is available at: https://www.article19.org/resources/myanmar-scrap-cyber-security-draft-law-and-restore-full-internet-connectivity/.

[10] State Administration Council, Draft Cyber Security Law 2022, translation into English with annotated changes from the earlier draft at: https://freeexpressionmyanmar.org/wp-content/uploads/2022/01/Cyber-Security-Bill-2022-EN.pdf. For analysis and commentary on this draft, see Centre for Law and Democracy (2022), 'Myanmar: Note on New Draft Cyber Security Law', April, https://www.law-democracy.org/live/wp-content/uploads/2022/05/Myanmar.Cyber-Security-Analysis-English-.pdf; Access Now (2022), 'Analysis: the Myanmar junta's Cybersecurity Law would be a disaster for human rights', 27 January, https://www.accessnow.org/analysis-myanmar-cybersecurity-law/; Free Expression Myanmar (2022) 'Military's cyber security bill worse than their previous draft', 27 January, https://freeexpressionmyanmar.org/militarys-cyber-security-bill-worse-than-their-previous-draft.

7. Develop a coordinated strategy for business advocacy
8. **Engaging Business Through HRDD Processes:**
9. 8. Identify and engage with responsible companies
10. 9. Advocate for responsible investment and human rights respect
11. 10. Ask business to carry out a heightened human rights due diligence process
12. 11. Stress the importance of conflict analysis and local expertise
13. 12. Participate in meaningful consultation with responsible business
14. 13. Harness leverage to influence government and business relationships
15. 14. Discuss divestment options and responsible exit