Myanmar ICT Ecosystem Study - a summary

A publicly available summary of a confidential study commissioned by the Parties of the 15th July 2022 MOU between Telenor and the Centre for Research on Multinational Corporations (SOMO) on behalf of 474 civil society organisations.

February 2024

threefold

Table of Contents

The Myanmar ICT Ecosystem Study and this summary report have been prepared by Threefold Sustainability, who have been jointly commissioned by the Parties of the 15th July 2022 MOU between Telenor and the Centre for Research on Multinational Corporations (SOMO) on behalf of 474 civil society organisations. Threefold Sustainability is a sustainability consultancy with expertise on business and human rights and the ICT sector.

The conclusions of this report represent Threefold Sustainability's best professional judgement and while good faith efforts have been made to ensure the accuracy of the information contained in this report, the report relies on data provided by third parties and its completeness or correctness cannot be guaranteed. The authors are not liable for any errors, omissions, or consequences arising from the use of or reliance on the information contained in this report.

1. Introduction

In July 2021, 474 civil society organisations raised a complaint against Telenor ASA with the Norwegian National Contact Point of the OECD contending that the company had failed to observe the recommendations of the OECD Guidelines for Multinational Enterprises in its disengagement from Myanmar through the sale of Telenor Myanmar Ltd.[1]

Following on from a Memorandum of Understanding agreed in July 2022,[2] the Parties to the complaint jointly commissioned an independent Information and Communications Technology (ICT) Ecosystem Study to enhance the understanding of risks associated with digital footprints and surveillance in Myanmar, including with regards to telecommunications data and equipment, and how these risks may evolve. The scope of the study did not consider other state-initiated misuse of digital services to, e.g., spread misinformation or to restrict access to information.

The full study remains confidential to the Parties and is based on publicly available reports, analysis and online resources accessed between June and December 2023 and approximately 20 interviews with representatives from civil society, academia, international organisations and the ICT sector. This is a public summary report of the study.

The topic of government surveillance and digital footprints is a sensitive one, in particular in the context of conflict affected and high-risk areas (CAHRAs)[i], such as Myanmar. While it was important to provide this public summary report of the overall study, details relating to specific circumstances in Myanmar as well as descriptions of different surveillance methods are not included here.

Human rights impacts of digital surveillance

The Global Network Initiative's (GNI) and Business for Social Responsibility's (BSR) Across the Stack Tool "Human Rights Due Diligence Across the Technology Ecosystem"[3] provides an overview of the different actors operating in the technology ecosystem and the high-level human rights issues most relevant to each part of the ecosystem. In CAHRAs in particular, impacts on the human rights of individuals from digital surveillance can be extremely severe and include:

- surveillance leading to violation of the right to privacy – whether of communications, relationships, opinions, or home;
- surveillance having a chilling effect on freedom of expression and freedom of association and movement, leading to self-censorship of expression, opinion, religious practice and participation in protests;
- surveillance leading to arbitrary arrests and detention, torture, inhumane and degrading treatment, and extrajudicial killings;
- surveillance used to reinforce discrimination including facilitating forced labour of ethnic minorities.[4]

According to the Office of the High Commissioner of Human Rights (OHCHR), since the coup in February 2021, "a seemingly endless spiral of military violence has engulfed all aspects of

[i] The term Conflict Affected and High Risk Areas (CAHRAs) used throughout this report should be broadly interpreted, based on the explanations and definitions from, for example OECD Due Diligence Guidance; the UNDP and UN Human Rights Working Group Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide; and the European Commission recommendations on the identification of conflict-affected and high-risk areas.

life in Myanmar. [...] Analysing the use of violence by the military against individuals opposing their power and the civilian population at large, clear patterns emerged demonstrating a continuous escalation in terms of number, type, intensity, and brutality of attacks."[5]

One of the tools available to the military junta is digital surveillance. It has been widely reported that the junta's opponents have been identified, for example, through public posts and sharing of content critical of the junta;[6] monitoring of their financial transactions;[7] and information found on mobile devices seized at checkpoints,[8] at protests[9] and in random checks.[10] Freedom House's 'Freedom on the Net 2023' report describes how in the worst cases, these scenarios have led to arrests, jail terms, torture and even death.[11]

2. Different digital actors and the data they collect

An individual's digital footprint is built up of personal information and data collected, stored, shared and used by a multitude of different organisations. Different actors in the ICT ecosystem are involved in collecting the personal data of their customers and users, and/or providing technology that can be used to enable other organisations to collect, store, share and use personal data.[ii] These actors include:

- communications and internet service providers;
- social media platforms and other services that allow user generated content;
- apps such as messaging, delivery, ride hailing, gaming, keyboard and donation apps;
- cloud service providers providing infrastructure, platform and software as a service;
- digital payment platforms that are either bank-led, telecoms-led or led by other/independent organisations:[12]
- providers of surveillance technology (hardware, software, services) either with the intended purpose of surveillance and/or with the potential for misuse for surveillance purposes. This includes providers of: CCTV equipment and systems; telecoms network equipment and managed services; lawful intercept solutions; spyware and device forensics; and drones.

Key facts about connectivity and internet use in Myanmar

In Myanmar, as of January 2023, there were:[13]

- 23.93 million internet users, equating to an internet penetration of 44%
- 64.6 million mobile connections, equating to 118.8% mobile penetration but with many people having more than one connection
- 90.3% of mobile connections were broadband (3G, 4G, 5G)
- 1GB of data cost $1.11, equivalent to 1.17% of average income
- 33% of web traffic was by laptop and desktop and 67% by mobile phone, with 90% of this originating from android devices

[ii] The Global Network Initiative's (GNI) and Business for Social Responsibility's (BSR) Across the Stack Tool "Human Rights Due Diligence Across the Technology Ecosystem" provides an overview of the different actors operating in the technology ecosystem and the high-level human rights issues and due diligence questions that companies in each part of the ecosystem should consider.

- 29% of over 15-year-olds have a mobile money account, with 36% having an account with a financial institution

As of October 2023, there were over 21 million Facebook users, almost 2 million Instagram users and almost 20 million Messenger users.[14]

There are also many other industries that collect, retain, share and use personal information and therefore contribute to individuals' digital footprints (and with the potential for access by State authorities for surveillance purposes). Users themselves also directly place personal information into the public domain through their own posts, likes, comments, tags and other user generated content that may be gathered by the authorities through open-source intelligence (OSINT).

The majority of ICT ecosystem actors will routinely collect, retain, use and share personal data for business purposes and/or if legally required to do so, with many providing at least some information on what personal data they collect within publicly available privacy policies. The length of time that a company retains personal data can vary considerably by company, country and data type - as does company transparency about these practices, as can be seen from, for example, Ranking Digital Rights' research.[15]

The people interviewed for this study consistently identified certain types of data as being particularly sensitive and high risk in the Myanmar context. These were:

- real-time location data;
- biometric data; and
- data held by companies that have a physical presence (such as infrastructure, offices and employees) in the country because – as well as jurisdictional considerations – this offers greater leverage to the junta to demand access to this information.

3. Surveillance of digital footprints

The UN Office of the High Commissioner of Human Rights has stated that, in Myanmar, shortly after the coup, the military "unilaterally amended and instrumentalised the legal framework to stifle free expression, justify arbitrary deprivation of liberty, and deny thousands of activists, journalists, and human rights defenders due process and fair trial rights."[16] In 2024, the different laws relating to surveillance powers are broad and vague in scope in a way that can be used to justify nearly any type of violation of privacy and freedom of expression.[17]

The study identified the following in relation to digital surveillance in Myanmar:

- It should be assumed that Lawful Intercept (LI) capability is likely active in at least the networks of the four mobile operators.[18] This would mean that, for example, mobile telephony calls[iii], text messages, interception related information (IRI)[iv], and device location (by cell tower ID) can be intercepted in real-time. Shutdowns of internet services, which remain frequent in Myanmar, force people to rely on 2G communications, increasing risks from LI facilitated surveillance.[19] It is important to note that LI can also be used to intercept roaming traffic under certain circumstances, i.e., that of a person using their Myanmar SIM card abroad and calling a number in

[iii] Note: this does not include Voice-over-IP (VoIP), such as those over messaging apps like WhatsApp or Signal.
[iv] Intercept Related Information (IRI) consists of information about targeted communications, including destination of a voice call (e.g., called party's telephone number), source of a call (caller's phone number), time of the call, and duration.

Myanmar, and of a person using a foreign SIM card in Myanmar calling a local number in Myanmar. If the calls are made with VoLTE[v] (and the Myanmar operator and the foreign operator have a VoLTE roaming agreement in place), there is a possibility for intercept of all calls.

- It is known that the junta have requested historical data from mobile operators,[20] which can pertain to, for example, subscription data, call detail records (CDR)[vi] and location information. It should be assumed that this and other type of user data is also being requested or accessed from other locally operating digital services, such as digital banking services, VPN or Burmese keyboard apps.[21]
- Digital financial transactions, including mobile money transfers, are being monitored and new banking and payment platform Know-Your-Customer (KYC) requirements mean they can be traced to individuals.[22]
- The junta are actively monitoring people's social media activities, potentially with the use of purpose-built OSINT tools,[23] and by infiltrating private profiles and groups and relying on informants, especially in popular applications such as Facebook and Telegram.[24]
- There are credible reports that the junta are utilising forensic spyware on devices that have been confiscated,[25] meaning all live and even deleted activity on the device can be compromised. This information can also be used to impersonate the device owners in order to gather information from others.
- There are also indications that the junta may be in possession of tools to remotely infect devices with spyware that can access all activity on those devices and potentially around them.[26] This is also a risk for exiled Burmese activists.

It is challenging to ascertain how widely and systemically these surveillance methods are being used; by which bodies of the State Administrative Council (SAC); or how the situation may evolve. In 2023, the Myanmar junta ramped up the collection of biometric data, within and outside of a population census project,[27] for the purpose of introducing an electronic ID (eID) which could then be used in SIM card registration.[28] The junta have also had discussions with the Indian government to learn about the roll out of the Indian 'Aadhaar' eID system[29] and with Chinese officials on replacing national ID cards with eID smart cards.[30] These efforts, together with the continuing roll-out of CCTVs across the country,[31] could indicate plans to put in place a more sophisticated surveillance system. This will not be a simple task in the Myanmar context where resistance to the junta remains determined[32] and significant time, money and resources would be required.

4. Risk mitigation and remedy

The Office of the High Commissioner for Human Rights (OHCHR) has noted that victims of targeted surveillance have had little success in obtaining recognition of the harm suffered, let alone remedies for such harm.[33] Particular challenges relating to remedy in the ICT sector have also been recognised by the work of the OHCHR's B-Tech project which has studied

[v] LTE stands for Long Term Evolution or 4G. 4G/LTE networks carry data only and voice is transmitted as Voice over IP / Voice over LTE (VoLTE).
[vi] Call detail records (CDRs) are attributes of a mobile telephony call or a text message (SMS) such as source number and destination number, time, duration, routing, cell ID (the base station where a call is connected) and completion status of calls and texts (dropped calls) and typically dozens of usage and diagnostic information elements. As opposed to IRI, CDR is historic information and available without lawful interception.

remedy aligned to the UN Guiding Principles on Business and Human Rights in the sector. Aside from the challenge of connecting a specific case of harm to the technology or actions of a specific ICT company, B-Tech has suggested that technology companies can "enhance the functioning of remedy ecosystems by empowering affected people and groups and their representatives" by "raising awareness about the ways that different technologies are used, […and being] open with people about the human rights implications of different design features."[34]

One of the objectives of the study was to provide input to the exploration of a 'digital security relief mechanism' and in particular the role such a mechanism could play in mitigating risks. A 'digital security relief mechanism' is understood to mean a fund of some kind, focused on reducing risks relating to digital footprints.

Interviewees for the study had a variety of views on what such a mechanism could offer. Although human rights defenders (HRDs) are increasingly aware of the risks relating to digital footprints and the steps they can take to help to reduce risks to their safety and security, many lack the resources to be able to use all technical safeguards available. There is also a considerable need for greater digital security awareness for the wider population. Interviewees also raised the need for resources to support the work of Burmese HRDs, journalists and academics both inside and outside the country.

There are practical challenges in the Myanmar context to implementing a digital security relief mechanism, among them ensuring the right support reaches the right individuals and groups without increasing the risks they and others may face.

5. Recommendations

The study makes the following recommendations:

For all ICT companies

- Establish robust policies and systems in relation to privacy and surveillance, based on internationally recognised laws and standards for human rights, including the UN Guiding Principles on Business and Human Rights. These should reflect the different roles, responsibilities and impacts that the different actors in the ICT ecosystem have, as well as potential mitigation measures. For example, the policies and systems that providers of surveillance technology should put in place to ensure their products are not misused by governments or other actors are different from those that should be implemented by communication and internet service providers in responding to demands from governments.
- Linked to the above, there is also an opportunity for ICT companies to work together and with other stakeholders to develop due diligence guidance focused specifically on privacy and surveillance. This guidance could map out the different risks, impacts, responsibilities and mitigation measures and identify good practices for different actors in the ICT ecosystem.
- Ensure that country human rights impacts assessments are informed by the perspectives and expertise of rights-holders from the country in question.
- Transparently communicate the findings of human rights due diligence processes (HRDD) and the actions taken to prevent and mitigate risks as a result of those findings.

- Provide details to users of what personal data is collected by the company (including data retention periods at the country-level if relevant) and how this data can be shared with the authorities. Support civil society actors' understanding of data collection, technology, surveillance mechanisms and how these may evolve.
- Provide contextual information relating to authority requests for customer / user data beyond just statistical reporting to help stakeholders make more informed decisions about their ICT use.[35]
- Advocate for the development of rights-respecting laws that clearly define how and by whom surveillance can be authorised; under what narrowly defined circumstances; and with what independent oversight.
- Ensure that the human rights impacts of potential country exit / disengagement are considered as part of human rights impact assessments conducted at market entry, particularly in relation to conflict affected and high-risk areas. This should include identifying steps that can be taken to minimise risks at potential future exit (e.g., data minimisation).
- Include human rights considerations and exit scenarios within the company's crisis management planning and regular crisis exercises with a particular focus on operations in CAHRAs.
- Conduct dynamic and enhanced human rights due diligence in relation to operations within CAHRAs, including designing processes for rapid HRDD for complex and fast-evolving situations and identifying most at-risk and vulnerable rights-holders.
- Proactively identify ways in which the company can support users' digital safety and security generally and in relation to the specific circumstances facing users in CAHRAs through, for example:
    - offering services and features that support digital safety and security (examples include Nord VPN's free emergency VPN offer[36] and Facebook's safety feature enabling users to quickly and easily lock their profiles.[37]);
    - establishing security-by-design processes for new products and services (taking into account the specific situation and risks within the country);
    - supporting wider initiatives to build digital safety and security understanding amongst users, in particular those rights-holders at greatest potential risk;
    - providing financial and material support to civil society and academic research that aims to build understanding and highlight human rights abuses using ICT;
    - putting in place operational level grievance mechanisms that would allow at-risk persons to both make contact and securely communicate with the company, and access individual remedy.

For Telenor

To the extent relevant, all of the above recommendations are also recommendations for Telenor as an ICT company. In addition:

- Continue to implement the findings of the Myanmar exit internal learning process[38] and transparently share:

- how the process has impacted the company's policy framework and internal procedures and how these changes are being implemented in existing operations;
- how and where the company is sharing its experiences and learnings with others;
- progress of training for Board members; and
- how the company has evolved its engagement with civil society and investors.

For the Parties (Telenor and the complainants)

> As part of future discussions and exploration of a potential digital security relief mechanism consider the risks, practicalities and potential governance relating to such a mechanism.

> Explore what role the Parties – together or independently – could take in relation to remedy more broadly, in particular:
  - the development of guidance for responsible exit / disengagement informed by this case; and
  - greater multistakeholder collaboration to consider remedy generally within the ICT sector.

For civil society, academia and research organisations

> Continue to advocate for rights-respecting legal frameworks, for example, the regulation of spyware in particular is a focus at the time of writing.[39]

> Continue to support activists and HRDs with their technology and digital security training needs with the objectives of not only being able to better protect themselves from risks, but also to effectively engage with ICT companies and hold them to account.

> Focus research efforts on building further understanding of the methods of surveillance being used by the junta in Myanmar, in particular methods that are known to be at their disposal such as the use of lawful interception, CCTV systems and targeted spyware.

> Two areas that could be considered for research more broadly are: the use of data brokers for surveillance purposes and the potential misuse of cloud services in enabling more sophisticated, AI-based surveillance systems.

For multilateral organisations and governments

> Ensure that any ICT-sector related financial and development support to governments in CAHRAs is conditional on the implementation of rights-respecting legal frameworks and oversight.

> Consider the human rights risks and impacts of financing and supporting ICT infrastructure development in CAHRAs, including, for example, digital ID or banking systems or training for crime prevention techniques.[40]

> In addition to robustly enforcing existing sanctions, conduct human rights impact assessments of sanctions, considering how impacts may evolve in the short, medium and long term.

- Provide financial and material support to civil society, independent journalism and academic research that aims to build understanding and highlight human rights abuses by authoritarian states using ICT.

End Notes

[1] NCP Norway (2021): NCP accepts submission, offers good offices to the parties
[2] NCP Norway (2022): Update in specific instance – MoU
[3] BSR and the Global Network Initiative (2022): Human Rights Due Diligence Across the Technology Ecosystem
[4] Access Now, Business & Human Rights Resource Centre, and Heartland Initiative (2022): Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors
[5] UN Human Rights Office of the High Commissioner (OHCHR) (2023): Situation of human rights in Myanmar - report
[6] Freedom House (2023): Freedom on the Net – Myanmar
[7] Radio Free Asia Myanmar (2023): Myanmar shutters 700 mobile bank accounts suspected of funding anti-junta forces
[8] Ibid. Freedom House (2023)
[9] Free Expression Myanmar (2020): No Permission to Protest
[10] Myanmar Centre for Responsible Business (2022): The Right to Privacy in the Digital Age: Experience from Myanmar
[11] Ibid. Freedom House (2023)
[12] Ei Nandar Kyaw, Myanmore (2022): The revolution of Myanmar fintech : mobile payment applications
[13] Datareportal (2023): Myanmar
[14] Social Media users in Myanmar - October 2023 | NapoleonCat (accessed in December 2023)
[15] The 2022 Ranking Digital Rights Telco Giants Scorecard and Ranking Digital Rights - The 2022 RDR Big Tech Scorecard – see question P6.1 in particular
[16] Ibid. OHCHR (2023)
[17] The study looked into powers given to the authorities in: Telecom Law (2013), Narcotic Drugs and Psychotropic Substances Law (2018), Counterterrorism Law (2023), Law Protecting the Privacy and Security of Citizens (2017), Electronic Transactions Law (2021), and draft Cyber Security Law (2021). Analysis and translations of many of these laws are available from: Free Expression Myanmar: Laws
[18] Phuy Phuy Kyaw, Open Technology Fund (2020): The Rise of Online Censorship and Surveillance in Myanmar
[19] Myanmar Centre for Responsible Business (2022): Private Security Companies in Myanmar, and Interviews
[20] See Telenor: Handling access requests from authorities (accessed in October 2023)
[21] Ibid., Radio Free Asia Myanmar (2023)
[22] Frontier Myanmar (2022): Junta weaponises digital banking transition to starve resistance funding
[23] Intelligence Online (2022): Kremlin's favourite OSINT expert helps Russian plans in Myanmar
[24] Fanny Potkin and Wa Lone, Reuters (2021): Insight: 'Information combat': Inside the fight for Myanmar's soul and interviews
[25] International Crisis Group (2021): Myanmar's Military Struggles to Control the Virtual Battlefield
[26] Securelist by Kaspersky (2019): New FinSpy iOS and Android implants revealed ITW and interviews
[27] Myanmar Now (2023): Myanmar junta launches pilot census
[28] Ibid. MCRB (2022)
[29] Ministry of Information of Myanmar (2023): MoIP Union Minister seeks Myanmar-India cooperation in e-ID system
[30] Radio Free Asia (2023): Junta enlists China in changing Myanmar IDs to biometric smart cards
[31] Article 19 and Digital Rights Collective (2022): Who buys and controls the CCTV? Myanmar's slippery slope to mass surveillance
[32] Jonathan Head & Lulu Luo, BBC (2023): A turning point in Myanmar as army suffers big losses
[33] OHCHR (2019): Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pp.12-13
[34] B-Tech (2021): Access to remedy and the technology sector: a "remedy ecosystem" approach, p. 6
[35] There may be legal restrictions to what companies can disclose. See, for example, the Global Network Initiative's (GNI) Country Legal Frameworks Resource.
[36] Nord VPN: Emergency VPN program
[37] Meta: Facebook Introduces a New Safety Feature in Myanmar
[38] Telenor (2023): Telenor publishes learning outcomes from Myanmar engagement
[39] European Parliament Press release (2023): Spyware: MEPs call for full investigations and safeguards to prevent abuse
[40] Michael Safi, The Guardian (2021): EU provided crowd control training to Myanmar police units; Brigitte Bureau, CBC (2020): Canada funding migrant-blocking operations in countries with poor human rights records; Access Now (2022): Open letter: World Bank and its donors must protect human rights in digital ID systems