Myanmar Centre for Responsible Business

# The Right to Privacy in the Digital Age: Experience from Myanmar

The Myanmar Centre for Responsible Business (MCRB) welcomes the opportunity to provide inputs into the UN OHCHR report on the right to privacy in the digital age. MCRB's input focusses, inter alia on the following topics mentioned by the OHCHR:

- digital identity systems rolled out by States and companies;
- use of biometrics for identification and authentication;
- targeted and mass surveillance, including of journalists and human rights defenders;

Our inputs relate to experience gained from our work since 2013 on business and human rights in Myanmar, including digital rights. In 2014, MCRB commenced a Sector-Wide Impact Assessment (SWIA) of Myanmar's ICT Sector. This drew on methodology developed for MCRB's first two SWIAs on oil and gas and tourism, in which the UN Guiding Principles on Business and Human Rights (UNGPs) were central to the approach. The assessment, published in September 2015, analysed Myanmar's ICT policy and regulatory framework from the perspective of whether it protected human rights. MCRB also undertook research on the ground based on interviews with various stakeholders and rights holders, including companies, users, and regulators. The SWIA covered offline rights related to the rapid rollout of Myanmar's telecoms infrastructure, but also online rights with chapters on Freedom of Expression, 'Hate Speech', Privacy, Surveillance and Lawful Interception, and Cyber-Security.

In the following seven years, MCRB has worked with government, business and civil society stakeholders to take forward the recommendations in the assessment and respond to the many new developments, including those which have occurred since the military's seizure of power from an elected civilian government on 1 February 2021.

MCRB has approached this input on privacy in the digital age from the perspective of responsible business and the UNGPs. These require companies to undertake human rights due diligence to identify any human rights impacts which companies may cause, contribute to, or be linked to. MCRB seeks to identify and share examples of actual and potential risks to help businesses prevent and mitigate impacts.

Human rights risks, including but not limited to those relating to fundamental rights in the digital sphere, have been heightened for all companies operating in Myanmar following the military takeover on 1 February 2021, and not just for those in the ICT sector. For example, personal data held by companies such as personnel records, if obtained by public security forces, can lead to detention or torture, and even death. Our input identifies some examples which may be of relevance not only in Myanmar but also in other situations and is structured as follows.

## 1. Lack of human rights safeguards in the legal framework

There have always been significant risks in Myanmar to digital rights, such as privacy, freedom of expression, and access to information. This is due both to the lack of human rights safeguards in the legal framework for telecoms/ICT, and to provisions in the laws which are either vague or inconsistent with international human rights standards. This includes laws – or the lack of them – on issues such as lawful interception, cybersecurity, data protection and cybercrime. These gaps were analysed in MCRB's 2015 Sector Wide Impact Assessment[1] and updated in subsequent policy briefs.[2]

When undertaking human rights due diligence and risk assessments in Myanmar, companies therefore need to take account of the weaknesses in the legal framework and lack of human rights protection that it provides. In the absence of effective legal requirements, companies need to pre-emptively take preventative and mitigating steps through the adoption of good practice and guidance from other countries, and incorporating, applying and enforcing provisions in policies, contracts and standard operating procedures (SOPs) which draw on international human rights standards.

MCRB summarised some of these issues in the input it made to the UN Office of the High Commissioner on Human Rights in March 2022 concerning the High Commissioner's report on the practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies.[3] In that input, MCRB summarised the – unsuccessful - attempts made by MCRB, some companies and others, to introduce safeguards into the legal framework which could reduce the human rights risks for companies and impacts for rightsholders. Failure to incorporate human rights safeguards, in particular for lawful interception, contributed to Telenor's decision in 2021 to exit Myanmar.

### Use of visual/video surveillance and monitoring

There is no legal framework for use of visual/video surveillance in Myanmar, generally referred to as Closed Circuit TV (CCTV). CCTV and other security systems (e.g. alarms, entry systems, GPS trackers) can, in addition to capturing activities, also capture sensitive personal data, including in metadata. Some of the risks associated with this were identified in MCRB's February 2022 Baseline Study and Human Rights Risk Assessment of Private Security Companies in Myanmar.[4] For example, CCTV recordings can be accessed and reviewed by public security to identify those involved in peaceful protest.

In the absence of regulation on CCTV usage, MCRB recommended companies should:

- Consider whether deployment of CCTV or other recording equipment addresses a legitimate pressing need that cannot be addressed by other means.
- Ensure that CCTV is only used for designated purposes and legitimate aims, such as prevention of crime, and not, for example, to spy on employees, customers or neighbours.
- Ensure that CCTV deployment is proportionate to the need. Disable audio recording. Consider whether a live feed is sufficient, rather than recording.

---

[1] https://www.myanmar-responsiblebusiness.org/pdf/SWIA/ICT/complete.pdf
[2] https://www.myanmar-responsiblebusiness.org/pdf/2019-Policy-Brief-Myanmar-ICT-Legal-Framework_en.pdf
[3] https://www.myanmar-responsiblebusiness.org/news/guiding-principles-tech-sector.html
[4] Private Security Companies in Myanmar: A Baseline Study, Human Rights Risk Assessment and Recommendations, MCRB February 2022.

- Undertake a data protection impact assessment when surveillance cameras are deployed, camera positions changed or new technological capabilities such as automatic facial recognition are used.
- Where CCTV is in use, place clear signs in English and Myanmar to inform the public that they may be recorded.
- Control access to recordings. Establish SOPs including escalation to senior management to respond to any demands for data from public authorities. Seek to have requests for data put in writing. Do not give unrestricted access to public authorities to CCTV monitoring points.
- Provide access to recordings of individuals who have been recorded, on their request.
- Retain CCTV footage for as short a time as possible and not more than 30 days, unless it is being used as criminal evidence, or shows evidence of human rights abuses and may be useful to those seeking redress.
- For scenarios involving peaceful protest, consider adopting SOPs to stop recording and immediately delete CCTV data where there is a risk that it will otherwise be used by the authorities to arrest those exercising their right to freedom of expression

MCRB also identified the 12 Guiding Principles of the Amended Surveillance Camera Code of Practice, UK Government, December 2021 and the template for a data protection impact assessment for surveillance cameras developed by the UK Information Commissioner Office and the Surveillance Camera Commissioner as useful tools that could be applied by companies in Myanmar. However, this seems to be an under-scrutinised area of technology use that would benefit from guidance by digital rights experts.

### New legal frameworks relating to ICT

A draft cybersecurity law has been under preparation for several years in Myanmar. Shortly after taking power on 1 February 2021, the military regime sent a limited number of business associations a draft of the law for comment. MCRB prepared a document analysing elements of the draft law from a human rights perspective, including the rights to privacy and freedom of expression (both of which are contained in Myanmar's constitution). This document was provided to organisations, particularly businesses, who could respond to the call for comments and engage in advocacy on the draft law.

Perhaps in the face of significant concern expressed by businesses and others, rather than adopt the draft Cybersecurity Law, the military regime instead incorporated elements of the draft cybersecurity law concerning privacy and data protection into amendments to an earlier Electronic Transactions Law (ETL)[5]. These amendments establish a requirement to protect 'personal data' and penalties for failure to do so. But they lack clarity on how collected data should be handled, such as provisions on the retention period, classification of the information to be stored and storage location. While representing the first time that Myanmar has had a legal framework for data protection, the provisions are not consistent with international human rights standards. Furthermore, very few people, including in the regulator, appear aware of the new legal requirements for data protection, or doing anything to enforce them.

In January 2022, a revised draft Cybersecurity Law was circulated for comment, having been partially amended to reflect comments received in February 2021, primarily from businesses. This included new

[5] See MCRB's consolidated version of the 2004 Electronic Transactions Law, as amended in 2014 and 2021, and unofficial translation, and pages 76-78 of Private Security Companies in Myanmar: A Baseline Study, Human Rights Risk Assessment and Recommendations, MCRB February 2022. Free Expression Myanmar's analysis of 18 February 2021 of 'Myanmar's new Electronic Transactions Law Amendment', highlights the relationship of these amendments to the provisions originally included in the draft Cybersecurity law.

provisions to criminalise the use of unauthorised Virtual Private Networks (VPNs). This would severely impact millions of people in Myanmar who make use of VPNs. Although the use of VPNs has privacy benefits, users are primarily connecting via VPN to access Facebook, which together with a number of media and other sites, is currently blocked by the military regime.

Given the dependence on Facebook by many small businesses, education and health providers, and social groups, any move to criminalise unauthorized VPN usage would have a widespread negative impact on many rights holders, including on their right to livelihood, right to health etc, particularly during the COVID pandemic, when Facebook was the main channel for public health information. MCRB compiled analyses of the impacts of the draft law, and shared these with businesses and other groups in support of advocacy against the proposed move, and then compiled and published statements from business associations.[6]

To date, it is unclear whether the draft law will be adopted in its current form, or amended to reflect the strong outcry against banning unauthorized VPNs. However, the experiences of encouraging business advocacy and collective action against damaging provisions in the draft cybersecurity law have shown that it is possible to align the defence of political rights, such as the right to freedom of expression, the right to information and the right to privacy, and advocacy on protecting economic, social and cultural rights, such as the rights to livelihood and health. By focussing on economic impacts, and amplifying the business voice, it may still be possible to have some impact on an authoritarian regime, at a time when advocacy based on political rights has no traction.

## 2. Low digital literacy and privacy awareness and practices amongst government and the public

MCRB, working with local partners including through the Myanmar Digital Rights Forum, has sought to raise awareness of privacy and data protection.[7] Privacy is not, however, a word which translates easily into Myanmar language, or culture.[8]

Lack of awareness of privacy and digital literacy and the absence of an effective legal framework for data protection can lead Myanmar people to place themselves and others at risk through the publication of personal data or a lack of attention to digital security. Although there is no data on the incidence of identity theft in Myanmar, it is a growing risk.[9] Myanmar's COVID-19 QR pass system was a victim of hacking, and open to identity theft and breaches of privacy.[10] The Directorate of Investment and Companies Administration (DICA) and Myanmar Investment Commission were hacked shortly after the coup, leading to the publications of documents from 120,000 companies, including the scans of personal ID of company directors.[11] Other Myanmar government sites have been regularly hacked, both pre and post-coup.

---

[6] Update on Draft Cybersecurity Law and its Impacts on Digital Rights and the Digital Economy, MCRB 15 Feb 2022

[7] Four meetings of the Myanmar Digital Rights Forum were held in 2016, 2018, 2019 and 2020. To celebrate Data Protection Day in January 2021, MCRB published a blog on Why Data Protection Matters! in English and Myanmar contextualising it for Myanmar audiences.

[8] MCRB translates privacy as ပုဂ္ဂိုလ်ဆိုင်ရာလုံခြုံမှု po-go-sain-ya loun-kyoun-hmu which translates literally as security of the person. but alternative translations include လျှို့ဝှက်ချက် (secrecy), ကိုယ်ရေးကိုယ်တာ (personal) or သီးသန့်တည်ရှိမှု (being separate)

[9] Myanmar Police Force helps investigate Facebook identity theft, Myanmar Digital Newspaper 24 June 2019

[10] Cyberattacks hobble Myanmar's COVID-19 QR pass system, expose massive security flaws, KrASIA, 1 October 2020

[11] Massive data trove from 120,000 Myanmar companies, KrASIAa 21 February 2021

Some privacy and data protection breaches by government departments take place as a consequence of their own actions, due to a lack of awareness. For example, the initial version of DICA's MyCo Companies Registry database allowed the full ID card/passport numbers of company directors to be seen in front of the paywall. Following feedback, including from MCRB, the ID numbers were masked to reveal only the last three digits of IDs, although full numbers are still available behind the paywall. [12]

Some publications related to candidates for election, including from the Election Commission, included sensitive personal data such as Citizenship Scrutiny Card (CSC) number and father's name. Such information is not needed by a voter. There are examples of government departments revealing similar personal data online, for example results of university entrance exams.[13] This is particularly sensitive in the current period, when those who decide to attend state education institutions are liable to be 'socially punished' by those who advocate a boycott.

The importance of keeping full personal identity numbers confidential has been recognized in the Aadhaar system which allows for the download of official 'masked Aadhaar' documentation to avoid identity theft.[14] Similar arrangements need to be made in Myanmar to reduce the publication online and offline of sensitive personal data including ID numbers.

Companies are also at fault do to failure to consider risks. MCRB has seen examples of Environmental Impact Assessment (EIA) reports uploaded online in which contain annexes of names of participants at public consultation meetings. In some cases participants had been required to fill in their ID card when they registered their attendance. While some project proponents and EIA consultants do not collect this data or recognise the need to mask it, not all are aware of the data protection breach. Furthermore, security in many public buildings including commercial premises require visitors to write their ID card or passport number in a publicly visible register, despite their being no security benefit from the acquisition of this information. These registers of sensitive personal data are inadequately protected, and available for scrutiny by the curious, or for capture by malicious actors.

Public officials, and the public in Myanmar need to be educated to better protect personal data, including the incipient data protection provisions in the amended Electronic Transactions Law. Applying the principle of **data minimisation** to the collection of personal data in instances such as these helps prevent the inadvertent disclosure of confidential information relating to an individual's personal identity. The International Association of Privacy Professionals identifies data minimisation as one of the core principles for reducing privacy harms "*There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject*."[15]

## 3. Digital ID cards, Biometrics, and SIM Card Registration

The absence of an adequate legal framework and safeguards for data protection has provided the backdrop to two ongoing initiatives to collective biometric and personal data which successive Myanmar

[12] MCRB Provides Comments to DICA Consultation on the Disclosure of Company Information, 31 January 2020. MCRB also advocated for the database improve its back-end functionality so as to automatically link the same individual to multiple directorships, without needed to reveal their personal ID.

[13] See for example the ID numbers, fathers' names and addresses of the candidates for 2022 admission to Bogalay Education Degree College

[14] https://www.uidai.gov.in/283-faqs/aadhaar-online-services/e-aadhaar/1887-what-is-masked-aadhaar.html

[15] https://iapp.org/resources/article/fair-information-practices/

governments have embarked on over the last decade. These are the introduction of a digital identity card, and SIM card registration. Developments on these and associated privacy and human rights risks, are outlined below.

### Introduction of eID

The ID4D initiative[16] has argued that digital identity is an important enabler of development, but should be implemented in line with the Principles on Identification for Sustainable Development (see below). If an individual lacks documentation, this can be a major barrier to realizing the right to citizenship, as well as other fundamental rights such as healthcare, education, employment and access to economic inclusion opportunities such as banking and mobile phones.[17]

According to the 2014 Myanmar Census, 27.3% of the population holds no identity document (it should be noted that the many challenges associated with the Census, the first to be conducted for decades, mean that even this figure may be an underestimate of the situation as it pertained in 2014). Obtaining a Citizenship Scrutiny Card (CSC) requires extensive evidential documents that are difficult and costly for many people to provide, such as 'household lists' which those living in informal settlements do not have. The current laws and their discriminatory implementation have made access to citizenship and identity documentation difficult and costly, particularly for ethnic and religious minorities.[18] Furthermore, some ethnic minority individuals report that their name, of an ethnic language origin, is mis-spelt in Myanmar language on the ID card, leading to alternate spellings on different documents. Statelessness is also a serious risk for many in Myanmar due to the interpretation and application of the 1982 Citizenship Law, which forms the central pillar of the current citizenship regime.

The Myanmar Citizenship Scrutiny Card contains a photo, fingerprint, and handwritten information covering:

| | | |
|---|---|---|
| • ID Number | • Race (lu-myo) | • Occupation |
| • Issue Date | • Religion (batha) | • Address |
| • Name | • Height | • Signature of Holder |
| • Father's Name | • Blood group | • Signature and rank of issuer |
| • Date of Birth | • Distinguishing Characteristics | |

Surprisingly, Gender is not a category included in the CSC.

The inclusion of Race and Religion is problematic. In addition to being unnecessary to determine identity, and potentially a source of harm through discrimination, some card holders report that what immigration officials write on the card differs from the individual's own expression of their ethnicity or religion.

The system is currently paper-based. If an individual loses their card, they need to return to their home township to obtain a replacement from the local immigration office, where details are held on paper files. With the weakening of local administration since the military coup, and the damage to local

[16] id4d.worldbank.org

[17] However some civil society groups globally have challenged the conclusion that this requires introduction of digital ID – see WhyID, Access Now https://www.accessnow.org/whyid/

[18] For further information on the application of Myanmar citizenship and identity laws, see A Legal Guide to Citizenship and Identity Documents In Myanmar, December 2018, Justice Base and Navigating with a Faulty Map: Access to Citizenship Documents and Citizenship in Myanmar, Institute on Statelessness and Inclusion, October 2021

administration offices, the system is very fragile. Replacements have to be signed for by senior officials. This can be costly, particularly for migrant workers who have to take time off to travel to their hometown.

The modernisation of the system, registration of individuals without ID, and introduction of digital identity cards has therefore been a priority for recent Myanmar governments, including the NLD Government in its 'Moe Pwint' project. In 2013, the Myanmar government announced that it would replace the paper National Registration Card (NRC) with a digital identification card ('Smart Card') to include biometric data**.**

In 2019, the government reported that it planned to seek international support to raise the $104 million needed to implement e-ID registration, and $286 million to supply smart ID cards,[19] and to seek parliamentary approval for this.[20] Many national governments exchanged views on eID with the Myanmar government; for example the Indian government offered to share the lessons of introducing the Aadhar system.[21] However, development partners were reluctant to provide funding, due to concerns around how ethnicity, religion and citizenship would be addressed, particularly relating to the Rohingya. Development partners also had concerns about the risks of exclusion of individuals in areas outside of state control, as well as being accused of facilitating the extension of central government control in areas which enjoy some form of autonomy or are seeking it. For example, the World Bank, when designing a 'digital government' support programme in 2018/2019 (now suspended), declined to be involved in any aspects of a digital ID programme.[22]

The NLD government established an e-ID System Working Committee in 2019 headed by U Thein Swe, the Minister of Labour Immigration and Population which reported into the e-Government Steering Committee. This was supported by six inter-ministerial sub-committees: Supervision; Planning; Laws and Regulation; Technical and Tender Guidelines Preparation; Funding; and Information and Communications. The structure was to be underpinned by implementation teams at State/region, township and ward/village level.

In 2019 the Austrian government was reported to be lending Euro 33 million to the Myanmar government to support the roll-out of a digital identity programme.[23] Attempts by MCRB to seek clarification from the Austrian Government and to advocate for human rights risks to be considered were unsuccessful. The Austrian government declined to engage, citing commercial confidentiality. Further reports suggested that this appeared to be an initiative undertaken by the partly state-owned Österreichische Staatsdruckerei (OeSD) (Austrian State Printing House). There were also reports of Myanmar parliamentary approval of a EUR 0.861 million grant and EUR 4.875 million zero-interest loan from Unicredit Bank for implementing public key infrastructure (PKI) for e-IDs for the 'population registry project'.[24] There has been no recent news about this loan.

---

[19] Parliament Pushes for Identity Cards to be Issued to IDPs Irrawaddy, 10 May 2019
[20] https://www.mmtimes.com/news/govt-begins-digitising-personal-information-id-cards.html
[21] Personal communication with MCRB
[22] https://projects.worldbank.org/en/projects-operations/project-detail/P167978
[23] https://www.mmtimes.com/news/myanmar-receive-austrian-loan-national-e-id-system.html
[24] Electronic population registration (e-ID) deserves warm welcomes **The Mirror,** 27 May 2020, p. 6 and Global New Light of Myanmar 28 July 2020, pg. 1

Since coming to power in 1 February 2021, the military State Administration Council (SAC) has continued to step up the issuance of CSCs to undocumented citizens, now named the Pan Khin Project[25]. They also are pursuing the plans for e-ID through broadly the same structures as under the NLD government.

The e-ID System Working Committee (still with six sub-committees) held coordination meetings on 26 October 2021 and 22 March 2022. At the October 2021 meeting, the SAC representative stated that, in accordance with the Sustainable Development Goals (SDGs), by 2030 every citizen should have official registration, including a birth certificate. It was also stated that the biometric and biographical data of each resident of Myanmar should be collected and linked to a unique number to enable the use of e-Government applications across a single platform.[26] These are aligned with the original objectives of the Committee established under the NLD government.

The October Working Committee was presented with studies of other countries' eID systems, including those in the region. It was recommended that biographic and **biometric data (fingerprints, IRIS, facial photo)** should be collected and stored in a database, and a **unique ID number** should be **generated randomly**.

The conclusion of initial discussions appeared to be that the project should prioritise the issuance of 'smart cards' to those who already have CSCs i.e. those already qualified as a citizen under the 1982 Myanmar Citizenship Law. As a consequence, those who would potentially most benefit from having a digital ID i.e. those without documents and who may or may not qualify as citizens may continue to be excluded, unless steps are taken to facilitate their inclusion in the system.

The March 2022 meeting[27] reported that implementation of e-ID will be carried out in two phases: 'Unit-ID' collection and 'National-ID' implementation. 'Unit-ID' appears to refer to pilot roll-out in the 81 townships of Yangon, Mandalay and Nay Pyi Taw Regions. An advisory group comprising local experts would be formed and could recommend on hiring foreign experts; equipment purchases would be tendered; laws would be amended as necessary. It was stated that **six items of biographic data** and **three types of biometric data** (iris, fingerprints, facial) will be collected from all people over 10 years old.

Although the summaries of the first two Working Committee suggest that they are seeking to learn from good practice elsewhere, it is unclear whether the Working Committee is incorporating good practice and intenational standards such as ID4D and the 2017 Principles on Identification for Sustainable Development into its approach. These are:

1. Ensure universal access for individuals, free from discrimination.
2. Remove barriers to access and use.
3. Establish a trusted—unique, secure, and accurate—identity.
4. Create a responsive and interoperable platform.
5. Use open standards and prevent vendor and technology lock-in.
6. Protect privacy and agency through system design.
7. Plan for financial and operational sustainability.

---

[25] Pan Khin Project: Union Minister Inspected Project Implementations, MITV, 4 July 2021 and Efforts being made to implement e-ID Population Registry, Global New Light of Myanmar, 20 August 2021

[26] Summary (in Myanmar) of the October 2021 meeting, Ministry of Immigration and Population website.

[27] Summary (in Myanmar) of the March 2022 meeting, Ministry of Immigration and Population website.

8. Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework.
9. Establish clear institutional mandates and accountability.
10. Enforce legal and trust frameworks through independent oversight and adjudication of grievances. [28]

Another source of good practice to which Myanmar could turn is the Modular Open Source Identity Platform (MOSIP) and its ten principles.[29]

To date, there is no information publicly available about what human rights and privacy safeguards will be applied to the eID system, including how data will be collected, stored and accessed.[30]

Concerning the planned **six** items of personal or 'biographic' data which are to be collected, MCRB understands that the six items under consideration by the Committee may be name, date of birth, place of birth, gender, father's name and mother's name.[31] However there is no information publicly available to confirm this. There has also not been a public comment to date on whether the Committee has adopted a policy of data minimisation.

A data minimization approach means that data on race and religion – currently in the Citizenship Scrutiny Card (CSC) - should not be included in an eID. Personal data that is not collected cannot be used to cause harm.[32] Given Myanmar's recent history, including discrimination and violence directed at certain religious and ethnic minorities, this is a risk. Information on race and religion is not necessary to establish a digital identity. It is not included in the Indian Aadhaar system which only includes **four** compulsory biographic or personal data: name, address, gender, and date of birth (and parent/guardian name in the case of children). Two others - mobile number and email - are optional in the Indian system.

Concerning conflict sensitivity, there is – unsurprisingly - no information available about how the Committee plans to approach the implementation of an eID scheme (and biometric SIM Card registration – see below) in the increasing number of areas of contested control. The choice of Naypyidaw, Mandalay and Yangon for rolling out 'Unit-ID' may be a tacit recognition of this challenge. However, the design of the eID system needs to take into account the views and interests of those in other areas included ethnic and contested areas which have, or seek, greater autonomy.

### SIM Card Registration and Biometrics

The issue of implementing eID is linked to the Myanmar government requirement for all mobile phone users to have a registered SIM card, and ambitions to establish a biometric database to achieve that. However it has not always been clear how the eID and SIM card registration programmes have been coordinated, if at all. As with plans for eID, there is little information and debate about SIM card registration, and privacy safeguards.

---

[28] https://id4d.worldbank.org/principles
[29] https://mosip.io/index.php
[30] See for example Protection of the Individual in the UIDAI System, Unique Identification Authority of India
[31] Personal communication, May 2022
[32] https://www.accessnow.org/cms/assets/uploads/2021/05/Data-Minimization-Report.pdf

The Myanmar government in 2014 announced a public consultation on mandatory SIM Card registration. This is a global trend: 161 countries require it as of 2021, of which 14 require biometrics.[33] In 2014 MCRB submitted comments calling for the human rights impacts to be considered.[34] This included the risk of excluding groups who do not have ID cards from access to essential services provided by phone, and the risk of providing an enhanced ability to track and monitor users, undermining their right to privacy and freedom of expression. This is a particular risk in countries such as Myanmar where legal safeguards for privacy and data protection are inadequate (see above). Since 1 February 2021, the human rights risks for users have heightened, since public security appear to be tracking user location based on SIM card use, leading to searches and arrests of opposition activists and journalists. [35]

Following the 2014 consultation, the government proceeded with the SIM Card registration requirement, based on individuals uploading a scan of their ID/passport or registering in a shop.[36] When the impact on users without ID became evident, some flexibility was provided in terms of documents which users could upload where they did not have a CSC or passport (e.g. attestation of identity from a local official).

The Post and Telecommunications Department announced that from 1 April 2019, each CSC card holder could only have a maximum of 2 SIMs per mobile operator (as there are 4 operators, this means a maximum of 8 SIM cards per person). However, a review of the registration databases held by companies in 2020 showed that in some cases several hundred SIM cards were registered to a single ID, probably by a reseller.[37] This risks an individual having their ID incorrectly associated with another user's activity. There were also suspicions that many SIMs were registered to fake IDs. Over 34 million unregistered and multiple-registered SIM cards were deactivated after 30 June 2020, during the COVID pandemic.[38]

In a resumed attempt to resolve the issue of multiple registrations and document fraud, the Post and Telecommunications Department (PTD) in 2019 developed plans to tender for a biometric database, capable of holding up to 70 million biometric records. It emerged that the costs of this database would be funded by the Universal Service Fund (USF), which was set up to increase access to mobile data for under-served areas and populations, but has not been spent on its intended purpose.[39]

Tender documents prepared by PTD in 2020 stated that the data to be collected would be 'name, left and right thumbprints, identity type, identity number and scan of identity card on both front and back sides', and possibly the person's father's name, date of birth and address. Copying the same data that are found on a CSC card for a database based on biometrics is not necessary, or consistent with a data minimisation

[33] https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws
[34] MCRB calls for Further Consideration of the Impacts of Requiring SIM Card Registration in Myanmar, 21 May 2014
[35] In May 2022, the SAC spokesman confirmed that they intended to require importers to register the International Mobile Equipment Identifier (IMEI) of devices. An IMEI is linked to the physical devices and remains the same throughout its life. It was claimed that this was to prevent import tax fraud. The significant lost tax revenues associated with mobile phone smuggling were documented by EuroCham Myanmar in 2019 amounting to $1.6 billion of an estimated $2.4 billion lost. It is unclear whether this registration will be connected in any way to the subsequent purchaser .Since phones may be shared, resold or passed down in families, it is not an accurate indication of the individual user.
[36] Mobile Users Must Now Register SIM Cards With Government, Myanmar Insider, 19 October 2016
[37] Announcement on systematic re-registration of SIM Cards, Myanmar Digital News, 23 February 2020
[38] Telecoms ministry says it has deactivated more than 34 million SIM cards Myanmar Now, 27 October 2020
[39] Myanmar diverts special telecoms fund to biometric database, Myanmar Times, 11 June 2020

approach. Privacy International wrote to PTD to raise concerns about the plans and the risk to privacy, particularly in the absence – at the time - of data protection provisions in Myanmar law. [40]

### Current Situation

As of mid-2022, MCRB understands that after several years of working in apparent isolation from one another, the Ministry of Immigration and Population (MIP) and the Ministry of Transport and Communications (MoTC) under the State Administration Council are working towards establishing a common biometric database that would both underpin a unique digital ID number and be used for SIM card registration.[41] The use of the Universal Service Fund has doubtless helped to bring the two Ministries together, in the absence of finding other funding for an eID system.

In the absence of development partner assistance, or a democratically elected government and parliament, it will fall to the de facto authorities and any private sector implementing partners to ensure that the system is implemented in a way which protects human rights including the right to privacy. Private sector implementing partners includes not only companies directly involved with the design and toll-out of the system, but also those who are supporting enrolment such as telecoms operators and other sellers of SIM cards where biometric and personal data could be collected.

This project is taking place at a time when the entire country can be considered a conflict-affected and high-risk area (CAHRA), and where the military regime is committing extensive human rights abuses.[42] Furthermore, there is lack of trust in the military regime and the civil service and an unwillingness on the part of much of civil society, and many businesses, to engage with it. This is likely to extend to unwillingness to participate in the planned 'local expert group' on eID, or in any wider public consultation, were one to be held.

If the SAC proceeds with the roll-out of an eID and SIM biometric database, it is therefore important that any private sector entities involved in its implementation should fully understand the human rights at risk. They should undertake heightened, conflict sensitive, human rights due diligence and pursue proactive engagement with rightsholders. They should advocate for the incorporation of the Principles on Identification for Sustainable Development, and MOSIP, into the approach so as to build rights protecting measures into the system. They should encourage transparency and effective communication, in support of an informed public debate on these important questions.

Above all, private sector entities should advocate for **a data minimisation approach,** and particularly one that excludes collection of data on race and ethnicity. They should also ensure that the system is inclusive, and accessible for persons with disabilities.

## 4. Additional privacy-related human rights risks since 1 February 2021

The following examples have been identified by MCRB as some of the other human rights risks relating to privacy which have emerged since the military coup:

---

[40] Myanmar: Dangerous plans for a National Digital ID and Biometric SIM Card Registration must be scrapped, Privacy International, 9 December 2019, Privacy International, updated January, March and June 2020, and January 2021

[41] MCRB personal communication with industry sources May 2022

[42] Myanmar: UN report urges immediate, concerted effort by international community to stem violence, hold military accountable, UNOHCHR 15 March 2022

- Public security demanding to review images recorded on a business' CCTV to identify peaceful demonstrators, or premises which decided to close during 'silent strikes'[43]
- Public security forces and other government officials demanding information about employees which participated in the civil disobedience movement (CDM) i.e. went on strike, or took part in demonstrations, for example by demanding attendance records.
- Workers facing risks on their daily commute and in their private lives of having mobile phones seized by security forces and searched for evidence of political activity, including using Facebook to share news about the civil disobedience movement (CDM), or using VPNs (despite their use not yet being illegal). Finding evidence of this on a phone could lead either to extortion, or detention and being charged with Articles 505 and 505A of the Penal Code[44], under which it is a crime to cause, or intend to cause, members of the government to be disobedient or disloyal.
- Erosion of privacy as a consequence of internet shutdowns since loss of 3G and 4G data services may leave only 2G GSM services (or none at all) which, as an old technology, are less secure and therefore vulnerable to interception and spoofing.[45]

Each of these examples has led to companies considering what steps they can take to keep workers and other rightsholders safe. Examples of preventive and mitigating actions include: removing video surveillance and CCTV cameras, switching off recording, or establishing protocols to ensure immediate deletion of data if demonstrations take place; taking care in the way staff absences are recorded and instructing security guards and other personnel not to provide information about individuals; and training staff in situational awareness and digital security, including the security provided by different forms of communication, and providing them with legal support, including pre-emptive briefings from lawyers on how to avoid detention.

MCRB has compiled and shared these and other examples with companies to support them in their human rights due diligence, so that they can do their best to keep workers, customers and other rights holders physically and digitally safe.

Myanmar Centre for Responsible Business

4 June 2022

[43] Silent strike empties streets in Myanmar on anniversary of coup, The Guardian 1 February 2022
[44] https://freeexpressionmyanmar.org/505a-act-of-revenge/
[45] https://www.eff.org/deeplinks/2020/06/your-phone-vulnerable-because-2g-it-doesnt-have-be