

PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

To: Seint Seint Aye, Head of Spectrum Management, Post and Telecommunications Department, Myanmar.

11th December 2019

Dear Ms Aye,

We are writing to express concerns and request urgent clarification regarding current plans for a "common database" requiring biometric identification from people wishing to register a SIM card, as reported in [The Myanmar Times](#) on 5 December 2019.

[Privacy International](#) (PI) is a registered charity based in London that works at the intersection of modern technologies and rights. Privacy International challenges overreaching state and corporate surveillance, so that people everywhere can have greater security and freedom through greater personal privacy. In a previous role, one of our staff worked with the Myanmar Centre For Responsible Business (MCRB) in drafting the ICT Sector Wide Impact Assessment in 2015. Privacy International submitted a shadow stakeholder report as part of the [Universal Periodic Review of Myanmar](#) in 2015.

You will recall the concerns raised by civil society when the Ministry proposed SIM registration in 2014. We understand that the agency now plans to require anyone buying a SIM to hand over their "name, left and right thumb prints, identity type, identity number and scan of identity card on both front and back sides". Additionally, the specifications continue, they may require the "father's name, date of birth and street address". We understand that prospective bidders are asked to ensure the centralised database is capable of holding up to 70 million biometric records.

As you will be aware, the processing of data, including collection, analysis, storing, sharing, must be prescribed by law. This could be data protection law or legislation passed specifically on the establishment of this system, providing responsibilities and obligations for processing activities and limited to that strictly and demonstrably necessary to achieve a legitimate aim. The law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the intrusion with someone's privacy.

Lack of Legal Safeguards

We are concerned with the apparent desire to push ahead with the plans without sufficient legal safeguards to protect people's privacy and security.

Myanmar does not have a data protection law in place. This means that the data processing required for the creation of a biometric subscriber database would occur in a legal void, so that information collected as part of registration today could be kept for an indefinite amount of time and used for different purposes in the future, as technology, corporate incentives, or governments change.

Further, Myanmar has yet to draft laws that govern the interception of communications by law enforcement. The telecommunication law adopted in 2013 provides extensive powers to the government including to access any information and telecommunications as well as to access telecommunication services for the matters relating national defence and security or public interest.

Request for Clarifications

Given these concerns, we ask that you answer the following questions:

- What problem is the biometric registration of SIM cards attempting to solve? What evidence is there that a "common database" is the solution?
- Was a feasibility assessment undertaken and if so, what was the conclusion?
- Was an assessment undertaken which determined that the development of the systems was necessary and proportionate to achieve a legitimate aim, as required by international law?
- Was a data protection and human right assessment undertaken to identify and understand the risks of such a scheme on the protection and enjoyment of fundamental rights and freedoms? And if yes, what mitigation measures were identified to address these risks?
- Will the company that ultimately provides the "common database" be responsible for personal data ownership?
- Which law(s) will effectively regulate the processing of personal data which this scheme requires?
- How long will the biometric data collected under these systems be retained for?
- As the proposal is for a centralised database, who will have access to the data contained within the database? And how will these permissions be regulated and overseen?
- What consideration has been given to the risks posed to people, especially minorities, if the biometric data was shared with other actors within Myanmar's security forces?

We thank you for your attention in this matter and look forward to your response.

Yours sincerely,



Lucy Purdon
Senior Policy Officer
lucyp@privacyinternational.org