To whom it may concern,

The **Mauritius Internet Governance Forum** (Mauritius IGF), hosted by Halley Movement, and the **Internet Society** welcome the opportunity to provide input to the proposed amendments to the ICT ACT for regulating the use and addressing the abuse and misuse of Social Media in Mauritius.

The **Mauritius IGF** is an initiative that fosters policy dialogue among stakeholders on issues of Internet governance. It offers a unique space for an amazing range of people to share information and develop solutions on key Internet issues.

Founded in 1992 by Internet pioneers, the **Internet Society** is a global non-profit organization working to ensure the Internet remains a force for good for everyone. Through its community of members, special interest groups, and 120+ chapters around the world, the organization defends and promotes Internet policies, standards, and protocols that keep the Internet open, globally connected, trustworthy, and secure.

In this joint submission we provide our comments, loosely structured around the questions asked in the consultation paper. Between our two organizations we provide both a local and regulatory perspective as well as a global technical perspective on the consultation.

14.1 - 14.2: Views on the present approach of self-regulation and alternative approaches

We appreciate the issues that the Mauritian government is facing while addressing illegal content and minimizing harm, but any approach that attempts to deal with this issue must respect the fundamental rights of privacy conferred to every individual. The proposed amendments would mean that all social media conversations of Mauritian citizens and visitors to Mauritius will be surveilled in neither a targeted nor proportionate manner.

We therefore call for the ICTA to consider the rights accorded to all Mauritian citizens to engage in private and anonymous communication without arbitrary surveillance or interception.

14.3 - 14.6: Views on the NDEC

We do not recommend the establishment of the National Digital Ethics Committee (NDEC), a powerful body whose role would be to assess and regulate or curtail harmful and illegal content on the Internet. We believe such a body would limit freedom of expression or intimidate the public from freely airing their opinions.

Any mechanism that would assess content would need to be accompanied by the highest safeguards. Those safeguards should include:

- Well-structured guidelines on the criteria of discerning how such a mechanism decides what is illegal and harmful.
- Regular review of those guidelines by a broad multi-stakeholder group to avoid unnecessary infringement of the freedom of expression.
- A method to keep the implementing body accountable and liable for overstepping its mandate.

Further, if a body or mechanism as powerful as the NDEC is being established, the law should detail a more comprehensive and elaborate way in which the proposed mechanism can ensure transparency, accountability, and confidentiality in terms of personal data.

14.7 - 14.8: Views on the Proposed Technology

The technical description raises several questions and concerns.

First, the definitions of ‘social media’ and ‘fake profiles’ need to be very precise and yet must consider the constantly changing landscape of social media tools. This creates a significant challenge.

Determining what constitutes social media traffic is difficult since it is often mixed in with additional types of traffic[1]. The system will therefore intercept passwords, two-factor tokens and other tokens that provide access to other sensitive information, like healthcare data or (critical) infrastructure. Since some social media platforms also involve commercial transactions, some small and medium enterprises (SMEs) have hosted their business there, and as a result confidential information (such as payment details) will be intercepted too. It is likely that some Mauritian businesses do not have a website and are only present on Facebook or other social media platforms.

Another example of confidential and private information that is hosted by social media platforms and which would be intercepted should this proposal go into effect is around a technology called “federated authentication” whereby some services rely on the security provided by their users logging in through social media accounts rather than having to have their own login and authentication services.

Secondly, the installation of a proxy and the distribution of a self-signed certificate for that proxy is a design that ***fundamentally undermines the security of the Internet for Mauritian users***.

There are several reasons for this:

1. There can be no technical guarantees that the private key associated with a trusted self-signed certificate can only be used to decrypt social media content. In fact, the ”proxy/certificate” mechanism that is proposed makes it possible for the government to masquerade as a citizen (or visitor) and/or as an online service.

[1] For more information about blocking and filtering content see RFC7754 “Technical Considerations for Internet Service Blocking and Filtering”, And “Internet Society Perspectives on Internet Content Blocking: An Overview”

For example, if banking information is tunneled through the proxy then details such as passwords can be decrypted and content such as payment amounts could be intercepted and altered. Since the mechanisms that attempt to filter social media traffic to the proxy are never precise, there will be content other than social media intercepted by the proxy. The mere fact that this is possible lowers overall trust in the system.

To make the same point in a different way: there is no way to make this mechanism trustworthy because, for example, a banking application would need to be supplied with cryptographic proof that the proxy cannot decrypt anything *except* social media traffic. There is no way to meet this technical requirement and therefore the use of a proxy poses a risk for all applications - not only banking applications - that are used by all Mauritian Internet users.

Because the proxy can be used to decrypt *any* type of traffic flowing through it and not just social media traffic, it could be a high-profile target for (state sponsored) cyber exploitation.

2. Requiring users to install self-signed proxy certificates has several issues:
    a. It assumes that the browser or the 'app' that is used to connect to the social media platform will present a pop-up notification that will allow users to install such a certificate. However, most browsers reduce the ability for users to override these settings in a convenient way, described below.

    b. Presenting a pop up with the choice to override a potential security alert is a huge security risk. This kind of notice is unfortunately best understood by well-informed users with technical competence on how to read cryptographic certificate data. When users get used to overriding these types of pop-ups or questions, they can easily be abused by third parties engaged in phishing.

    c. In the past, Google and Mozilla have sought to protect users by blocking certificates on their browsers to prevent the weakening of security for their users[2]. We can expect the same treatment here of any Mauritian proxy certificate.

3. Further in the proposed architecture, international travelers would find their devices tainted with 'spy certificates' and perhaps a proxy setting. Mechanisms to eradicate these certificates and settings would further complicate the user experience and put them at risk for phishing and other cyber-attack methods as they become accustomed to clicking through important pop-up warnings.

This all results in reduced overall security of the Mauritian Internet.

Summary

The technical solution presented in the 'Consultation Paper on proposed amendments to the ICT ACT for regulating the use and addressing the abuse and misuse of Social Media in Mauritius' undermines encryption and the general security of the Mauritian Internet by adding a proxy that indiscriminately decrypts all traffic that is routed through it. This type of encryption backdoor introduces vulnerabilities that can be exploited by others. The deployment of user certificates relies on methods that resemble the criminal behavior of phishers. Furthermore, the proxy can easily be avoided through the use VPNs or overlay networks.

Encryption is an important technology that helps Internet users keep their information and communications confidential and secure, and serves a crucial role in reinforcing the *personal security* of billions of people every day and the *national security* of countries around the world.

Any technical means to decrypt social media messages can be used to decrypt any other traffic and is therefore fundamentally untrustworthy.

Further, the establishment of a committee to assess and censor speech sets a precedent in limiting the fundamental rights of Mauritian citizens.

[2] See for instance Mozilla's statement.

We do understand the issues associated with disinformation on social media and urge you to engage with the local Internet stakeholder community to identify constructive and creative ways to deal with this issue.

Finally, we are strongly aligned with the joint civil society statement in response to your consultation signed by Access Now[3] and many other organizations and individuals. It makes similar points to our submission and stresses that the impact of the Mauritian regulator's proposed actions will go beyond its borders, raising global concerns.

Mahendranath Busgopaul
Secretary General - Halley Movement
Coalition
African Union ECOSOCC - Elected GA
Member
Director - Mauritius & IOS IGF

Olaf Kolkman
Principal - Internet
Technology, Policy,
and Advocacy
Internet Society

For more information, please contact ***media@isoc.org****.*

[3] https://www.accessnow.org/cms/assets/uploads/2021/05/Mauritius-ICT-Act-Submission.pdf