Mozilla and Google's Response to the Mauritian ICT Authority's call for comments on amendments to the ICT Act

Thank you to the Information and Communications Technology Authority (ICTA) of the Government of Mauritius for the opportunity to submit feedback on the proposed amendments to the ICT Act for "regulating the use and addressing the abuse and misuse of Social Media in Mauritius." We look forward to addressing issues in Mauritius, which, largely due to the country's dedication to open networks and transparent governance, was chosen as the home of the regional Internet registry for Africa. Our organizations are committed to fighting abusive and harmful content and we appreciate the opportunity to engage on the matter.

This comment details our concern with proposed amendments to Section 18(m) of the ICT Act, which would impose "technical enforcement measures" with the stated purpose of curtailing "identified illegal and harmful content." The amendments specify technical measures such as self-signed digital certificates that will be used as trust anchors, by which the Mauritian government can intercept, decrypt, re-encrypt and store Internet traffic data. We understand concerns about moderation of content in local languages raised in the consultation. The proposed approach would, however, have severe and disproportionate implications for privacy and security for Mauritian citizens, as well as others abroad, while doing little to address the stated concerns.

As proposed, the ICT Act's technical enforcement measures would work to undermine the trust of the fundamental security infrastructure that currently serves as the basis for the security of at least 80% of websites on the web that use HTTPS, especially those that carry out e-commerce and other critical financial transactions. The ICTA's proposal would thus not only put Mauritanian's privacy at risk but would also compromise the integrity and security of the system that Mauritius and many other nations depend upon for essential services. The result would be a less secure internet for Mauritian citizens, one that puts them at greater risk of fraud, identity theft, and surveillance.

In the past, when similarly dangerous mechanisms have been abused as proposed, whether by known-malicious parties, business partners such as a computer or device manufacturer, or a government entity, we've taken steps to protect and secure our users and our products.

The Internet Architecture Board (IAB), which helps support the global collaboration and development of Internet standards, published RFC 7754 - Technical Considerations for Internet Service Blocking and Filtering. This document highlights the many technical challenges for the ICT Authority's proposed approach, as well as unintended impacts and the limits of their effectiveness.

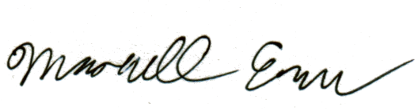
In addition, the Authority's proposed approach will not work with commonly used mobile devices that limit the use of certificates designed for interception. Similarly, such interception is not consistent with the use and deployment of technologies such as DNS over HTTPS, RPKI, and Encrypted Client Hello, all of which are critical to reinforcing Internet security and privacy. It has been shown that even passive enforcement devices, known as middleboxes,

have had a negative impact on Internet security. Such methods have introduced bugs and other problems and have hindered necessary and basic security improvements, like those of TLS 1.3.

As acknowledged in the IAB's RFC 7754, a strategy of blocking entire sites and IP addresses, while neither perfect nor fool proof, does significantly less harm than attempts to intercept, particularly at the network level. Blocking activity and speech however can still be harmful, and therefore operating within international frameworks for cross-border law enforcement cooperation and enhancing communication with industry can provide a more promising path.

We agree with the Authority's statement that the "proposed statutory framework will undoubtedly interfere with the Mauritian people's fundamental rights and liberties in particular their rights to privacy and confidentiality and freedom of expression" and urge the Authority not to pursue this approach. We are available to discuss any of the concerns mentioned in this submission.

Regards,



Marshall Erwin,
Chief Security Officer,
Mozilla Corporation

Email: merwin@mozilla.com
Phone Number: +1 650-903-0800
Address: 2 Harrison St #175, San Francisco, CA 94105, United States

Jointly submitted with Google