Comments on the Consultation Paper on proposed amendments to the ICT Act for regulating Social Media in Mauritius

By Ish Sookun

18 April 2021

Abstract

The Information and Communication Technologies Authority published a Consultation Paper on 14 April 2021 which contains proposals to amend the ICT Act. The ICT Authority proposes two frameworks and a set of tools to decrypt and archive Internet traffic for inspection purposes. The ICT Authority invited the public to comment on the Consultation Paper and to submit their comments by email by latest 5 May 2021 at 16h00. In this document, I comment on the **problem statement**, the **proposed frameworks** and the ***toolset*** mentioned in the Consultation Paper.

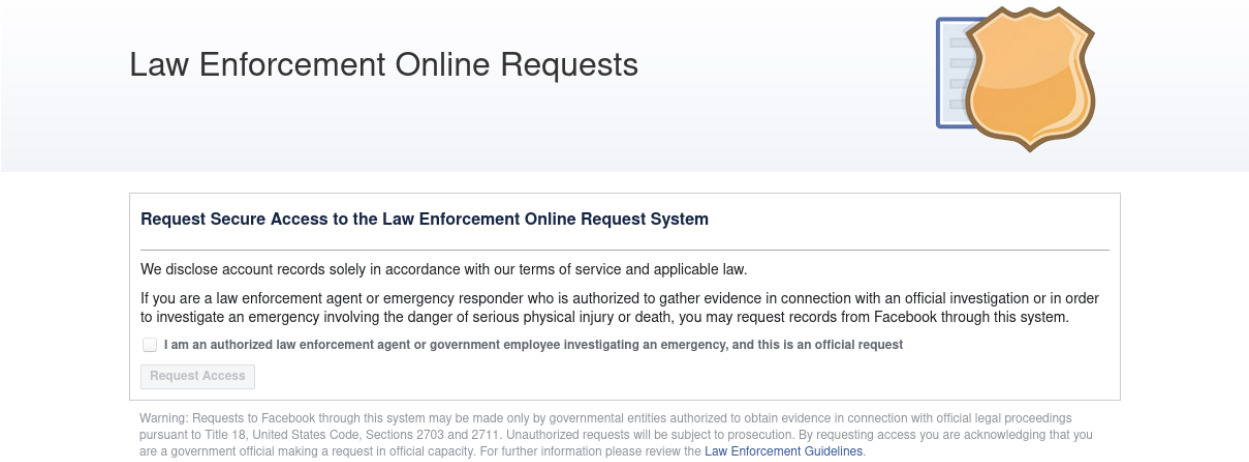
My name is Nitin K. Sookun. I'm also known as Ish. I work as a Systems Architect in a media group in Mauritius. I am an avid Internet user, a blogger and I volunteer in open source related activities both in Mauritius and outside the country. I have a keen interest in the advancement of the Internet in Africa & the Indian Ocean region.

Analysis of the Problem Statement

The examples of the incidents in India and Myanmar are based on rumours, which sound more of a societal problem. WhatsApp and Facebook provide communication tools. A rumour can circulate by any communication means, whether through a poster or a simple message transmitted to hundreds of people. Rumours will outlive technology. If there is no Facebook or WhatsApp, a malicious person can still find a non-tech way to spread a rumour. Banning these tools is not the solution. Providing factual and verifiable information are better means to counter rumours.

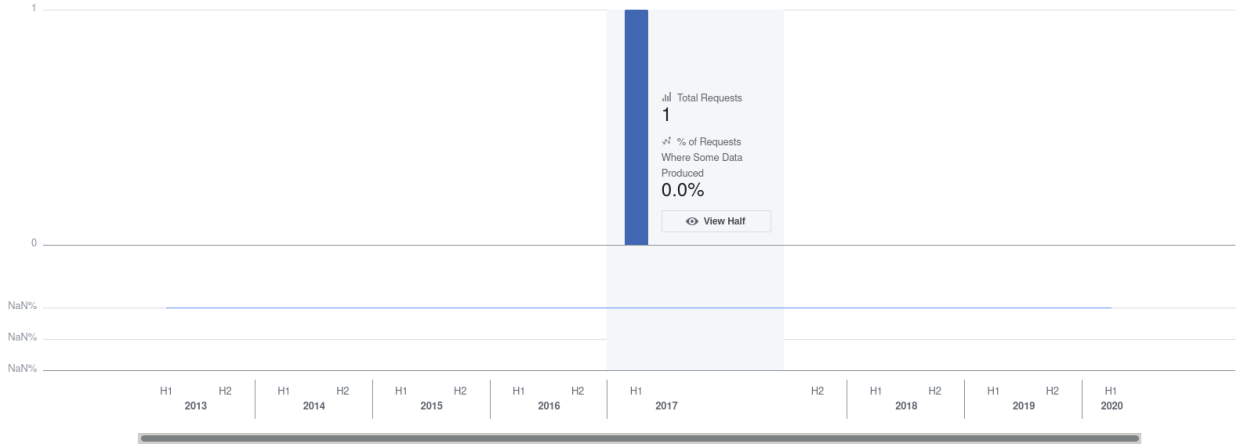
Also, rumours and fake news are not the same, but I believe the difference is not of interest to the ICT Authority here since both will be categorized as « harmful » under Section 18(1)(m) of the ICT Act.

Regarding the local context, the language barrier is mentioned. The Consultation Paper does not provide details on the methods that law enforcement bodies use to investigate and act on offensive content on social media platforms. Does an officer sign into Facebook ***using his personal account and reports a post*** or do law enforcement officers use the more proper channel established by Facebook to attend to law enforcement requests?



Screenshot taken from facebook.com

The Facebook Transparency Report[1] shows that in recent years there was only **1 request** made by Mauritius.



Screenshot from the Facebook Transparency Report

[1] https://transparency.facebook.com/government-data-requests/country/MU/jan-jun-2017

Does the ICT Authority have documents to support that requests to Facebook were made through proper channels? Does the ICT Authority have the answers from Facebook to support that there is indeed a language barrier when reporting offensive/abusive content written in creole?

Facebook mentions the Mutual Legal Assistance Treaty in its guidelines[2] about international legal process requirements. An officer of the Cybercrime Unit of the Central Criminal Investigation Division (CCID) on a radio programme by Radio Plus, Le Grand Journal[3] on 28 January 2016 mentioned that most of the requests that they send to Facebook are entertained by the latter. At 36 min 30 sec the officer mentions that content from Facebook is taken down through a collaboration with CERT-MU.

Therefore, it appears that the Mutual Legal Assistance Treaty is working and Mauritius is getting information from social media companies despite not having a regional office. Are we looking at a non-existent problem then? Or the officer misled the population and gave us fake assurances on cooperation between the CCID and Facebook?

Did the ICT Authority thoroughly study the investigation methods of our local law enforcement officers to find whether they have shortcomings? **Is it possible that the problem is not non-cooperation, slow response or language barrier by social media companies, but in fact simple human errors and judgement when investigating?**

Data on Cybercrime in Mauritius

The data provided about cybercrime in Mauritius is not adequate. It only shows the number of incidents reported via the Mauritian Cybercrime Online Reporting System[4] (MAUCORS). A total of **2,051 incidents** were reported between January 2020 and January 2021.

We cannot know how many of these reported incidents reflect actual cases.

There is no data on the number of cases currently being investigated, pending or completed. No data on cases involving different social media companies, e.g Facebook/WhatsApp, Twitter, YouTube, Telegram, etc. There is no reference to actual cases and certainly nothing to show problems that might be delaying investigations.

---

[2] https://www.facebook.com/safety/groups/law/guidelines
[3] https://podcasts.defimedia.info/280116-le-grand-journal
[4] http://maucors.govmu.org/English/Pages/default.aspx

If there is no data to show problems on social media or non-cooperation of social media companies then why is the ICT Authority proposing to amend the law?

The picture on cybercrime is unclear and poorly painted by Section 6.1 of the Consultation Paper.

Confusion in the ICT Act?

In Section 6.6 of the Consultation Paper it is mentioned that ***different stakeholders have different understanding*** of the ICT Act Section 18(1)(m) clause due to its very open-ended nature.

> *« The Authority shall take steps to regulate or curtail harmful and illegal content on the Internet and other other information and communication services. »*

Therefore, the ICT Authority acknowledges that this specific clause is open to interpretation. **Wouldn't it be better to amend the clause to make it concise rather than looking for technologies to censor the Internet based on an open-ended law?**

There is an overstatement of problems relating to social media in Mauritius with little to nothing to support an excessive, repressive and pervasive monitoring tool.

Comments on the Proposed Frameworks

Regarding the National Digital Ethics Committee (NDEC) there is no mention on who appoints the committee members. **Are they appointed by the Minister of TCI, the Prime Minister or somebody else in the government?**

The NDEC has complete freedom on deciding what is harmful. If an online press article exposes a government scandal and causes public outcry, the NDEC can deem it harmful to social harmony and instruct the technical unit to block the website.

There is absolutely nothing in these amendments that limit the application of censorship to social media only. Any website that publishes something deemed harmful by the NDEC can be subject to the law and thus censored.

Regarding the Technical Enforcement Unit, since that will be set up at the ICTA, naturally the team members will be employees of the ICTA. **Does it mean that the Enforcement Unit will operate under the administration of the ICTA Board which is appointed by the Prime Minister?**

In my humble opinion, neither the NDEC nor the Enforcement Unit instill public confidence. They do not bring clarity to Section 18(m) of the ICT Act but instead the powers are vested upon a few to interpret this section of the legislation in their way and execute as they deem fit. Efforts should have been made to make the wordings concise and reduce the broad interpretation of this law.

Comments on the Toolset

The ICT Authority will operate a proxy server that will **monitor all Internet traffic in Mauritius**. It will also decrypt HTTPS traffic for inspection purposes.

Without elaborating technical details, this means that when I type facebook.com in my web browser, the request will not be sent to Facebook servers but instead it will be sent to the proxy server at the ICT Authority. The request will then be sent to Facebook from the proxy server and the resulting page returned to my browser. Thereafter, when I type my username & password in the Facebook login form, those will be sent to the ICTA proxy server again, **where the information, i.e my username & password, will be copied & archived**, and then the ICTA proxy server will impersonate me and send the information to facebook.com in order to login. **Subsequently, all requests between my browser and Facebook will be intercepted by the ICTA proxy server, copied and archived.**

No. I do not agree to giving the ICT Authority my password.

In order for the ICT Authority to impersonate me, first the proxy server should impersonate facebook.com. To do so, the proxy server will have to generate a self-signed certificate for facebook.com and make my browser accept this is legitimate. I will be required to install a Certification Authority (CA) certificate in my browser to allow the proxy server to impersonate any website on the Internet and decrypt the information between my browser and the website. The Consultation Paper mentions social media but the technology works for all websites on the Internet.

Certification Authorities operate on a basic principle called the **chain of trust**. The Consultation Paper proposes the ICT Authority to break this “chain of trust” by doing what in cybersecurity terms is called a Man-In-The-Middle (MITM) attack.

I do not support the ICT Authority in doing what is generally regarded as illegal, unethical and pervasive.

It is mentioned in Section 13.1 that the public consultation is a driver to dispel the perception of a repressive measure and the ICTA wishes to avoid threats from social media companies as it happened in Pakistan when the government attempted to deploy similar mechanisms.

It is not only social media companies who will react to this repressive measure but also browser makers, businesses and other stakeholders operating on the Internet.

There is a high chance that major browser makers will prevent the ICTA CA certificate from being added to their browser's certificate store. This will render the whole operation of the ICTA futile.

The Consultation Paper only mentions the installation of the ICTA proxy server CA certificate in the browser to be able to access social media platforms. It does not elaborate on the technicalities of non-browser programs that also communicate with social media platforms using the HTTPS protocol.

Conclusion

Instead of trying to regulate social media using censorship tools, we should educate people about the Internet. The law enforcement officers should help in awareness and educate people on how to use the Internet in a better & safer way. Help people understand the law instead of scaring them with the law. Officers should also be better trained to investigate cybercrime cases.

Every time law enforcement officers intervene on radio or TV programmes, they focus on fine & imprisonment rather than giving proper advice on making the Internet a safe place. This should change. There should not be a fear factor when it comes to people hearing about the ICT Act.

Internet users should be empowered with the knowledge of the law, dangers & risks on the Internet, and understand netiquette, in order to avoid pitfalls.

The proposed amendments will cause more harm than good. People with malicious intentions will still be able to bypass ICTA's proxy server to incite hate speech, share offensive/illegal content or abuse politicians.

These amendments will directly hurt businesses and impact the economy, while taking away the rights of the citizens. The amendments should not be passed.