

Comments on Proposed Amendments to the Mauritian Information and Communications Technologies Act

May 2021



Centre for Law and Democracy

info@law-democracy.org

+1 902 431-3688

www.law-democracy.org

This Note¹ responds to 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 (Consultation Paper)² released by the Mauritian Information & Communication Technologies Authority (ICTA) on 14 April 2021. The Consultation Paper proposes amendments to the Information and Communication Technologies Act (ICT Act)³ to address the “abuse and misuse” of social media. Specifically, it proposes an approach which entails the routing of all social media traffic to and from Mauritius through a proxy server to be run by the ICTA, breaking any encryption provided by social media companies and allowing for official surveillance of all communications with a view to facilitating the enforcement of existing content restrictions in the ICT Act, along with new measures such as the blocking of offending websites. The content restrictions in the ICT Act already fail to meet international standards for restrictions on freedom of expression, but implementation of the approach proposed in the Consultation Paper would flagrantly breach Mauritius’ obligations to respect the rights to freedom of expression and privacy. These violations are exacerbated by the risk that the content-adjudication agency is unlikely to be independent of government and the fact that the technical enforcement agency is not independent.

This Note first debunks some of the Consultation Paper’s misleading justifications for the drastic proposals it puts forward. The next section starts by explaining the proposals in the Consultation Paper and then goes on to explain how those proposals, linked to existing legal rules, violate Mauritians’ rights to privacy and freedom of expression as protected under international human rights law, due to both the substantive restrictions they place on these rights and the manner in which those restrictions are enforced and sanctioned. The Note then outlines international standards calling for bodies which regulate freedom of expression to be independent of the government, and analyses the extent to which this is or

¹ This work is licensed under the Creative Commons Attribution-Non Commercial-ShareAlike 3.0 Unported Licence. You are free to copy, distribute and display this work and to make derivative works, provided you give credit to Centre for Law and Democracy, do not use this work for commercial purposes and distribute any works derived from this publication under a licence identical to this one. To view a copy of this licence, visit: <http://creativecommons.org/licenses/by-nc-sa/3.0/>.

² Available at: https://www.icta.mu/docs/2021/Social_Media_Public_Consultation.pdf.

³ Information and Communications Technologies Act 44/2001, https://www.icta.mu/docs/laws/ict_act.pdf.

is not the case with the bodies which will implement the new proposals. The Note goes on to explain why the proposals are unlikely to deliver effective solutions to the types of problems the Consultation Paper claims are prevalent in Mauritius. The Note concludes by putting forward some workable alternatives that Mauritius should consider pursuing to address the problems identified in the Consultation Paper, to the extent that they are indeed challenges for Mauritius.

The Consultation Paper's Misleading Justifications

The Consultation Paper's justifications for its extreme proposals significantly overstate both the harm of social media and the inability or unwillingness of social media companies to take measures to address that harm. First, the Consultation Paper states that social media companies' self-regulation "is exclusively based on their own acceptable usage policies irrespective of the domestic laws of individual countries" (paragraph 3.2; also see paragraph 6.10). This is false. Social media companies have taken down videos that complied with their usage policies but violated domestic law. For example, in 2012, Google blocked access to a video titled "The Innocence of Muslims" from Youtube in a few countries, including India and Indonesia, because the video was illegal in accordance with their domestic law; the video was left up elsewhere in the world because it was within Youtube's acceptable use guidelines.⁴ In 2020, Facebook blocked Singapore users' access to an allegedly false Facebook post to comply with Singaporean law even though the post did not incite violence or hatred and was thus within Facebook's content guidelines.⁵

More generally, the major social media companies have dedicated significant resources to addressing the most serious speech-related problems that take place on their platforms, such as hate speech, child porn and terrorism. Facebook employs around 15,000 content moderators who are tasked with identifying and taking down hate and other types of problematic speech.⁶ Twitter has suspended hundreds of thousands of user accounts for child pornography, detected through a combination of user reporting, dedicated monitoring staff and algorithms.⁷ A group of tech giants comprising Microsoft, Twitter, Facebook and Google have created the Global Internet Forum to Counter Terrorism (GIFCT), an industry-led consortium that seeks to prevent terrorists from exploiting social media.⁸ Consortium members cooperate through initiatives such as a shared industry

⁴ BBC News, "YouTube under new pressure over anti-Muslim film", 19 September 2012, <https://www.bbc.com/news/technology-19648808>.

⁵ Channel NewsAsia, "Facebook blocks Singapore users' access to States Times Review page", 18 February 2020, <https://www.channelnewsasia.com/news/singapore/facebook-blocks-singapore-users-access-states-times-review-pofma-12446952>.

⁶ Zoe Thomas, "Facebook content moderators paid to work from home", BBC News, 18 March 2020, <https://www.bbc.com/news/technology-51954968>.

⁷ Sean Sauro, "How social media goes after child porn: Tip led to Pa. Sen. Folmer's arrest", Penn Live, 20 September 2019, <https://www.pennlive.com/news/2019/09/after-former-pa-sen-folmers-arrest-experts-discuss-social-medias-role-in-child-porn-investigations.html>.

⁸ Stuart MacDonald, "How Tech Companies are Trying to Disrupt Social Media Activity", Scientific American, 26 June 2018, <https://www.scientificamerican.com/article/how-tech-companies-are-trying-to-disrupt-terrorist-social-media-activity/>.

database of pro-terrorist digital activity that ensures that if one consortium member takes down pro-terrorist content, all the other members can rapidly follow.⁹

The Consultation Paper's assertion that social media companies' acceptable usage policies apply "irrespective" of domestic law is also misleading (paragraph 3.2) because the content policies of the main companies – Facebook,¹⁰ Instagram,¹¹ Youtube¹² and Twitter¹³ – already include prohibitions that largely dovetail with the global consensus on classes of illegal speech including: violent content or incitement to violence; terrorism or incitement to or glorification of terrorism and other crimes, including impersonation; hate speech; and child pornography. Facebook's content policy¹⁴ and corporate human rights policy¹⁵ cite international human rights standards such as the *Universal Declaration of Human Rights*¹⁶ and the *International Covenant on Civil and Political Rights* (ICCPR).¹⁷

Just to be clear, CLD does not necessarily endorse these measures by social media companies and neither does it take the position that social media companies' policies and decisions are perfect or adequate. Rather, our point is that the government of Mauritius cannot justify the extreme measures it is proposing on the basis of inaccurate and overstated claims about the nature of the problem that needs to be addressed.

Another example of a misleading claim is the Consultation Paper's allegation that incitement of hatred through Facebook in Myanmar in November 2018 caused the Rohingya refugee crisis (paragraph 3.1). In fact, the proximate cause of the Rohingya refugee crisis was the August 2017 "clearance operations" by the Myanmar military in Rakhine State in retaliation for border clashes with Rohingya insurgency forces.¹⁸ Anti-Rohingya sentiment in Myanmar pre-dates the arrival of social media in the country.¹⁹ Facebook was indeed used to stoke anti-Rohingya sentiment in Myanmar, just as users take advantage of it to spread their views on almost everything, whether in the public interest or

⁹ *Ibid.*

¹⁰ Facebook, Community Standards, <https://www.facebook.com/communitystandards/>.

¹¹ Instagram, Community Guidelines, <https://www.facebook.com/help/instagram/477434105621119>.

¹² Youtube, Youtube policies, https://support.google.com/youtube/topic/2803176?hl=en&ref_topic=6151248.

¹³ Twitter, the Twitter Rules, <https://help.twitter.com/en/rules-and-policies/twitter-rules>.

¹⁴ See note 10.

¹⁵ Facebook, Corporate Human Rights Policy, 16 March 2021, <https://about.fb.com/wp-content/uploads/2021/04/Facebooks-Corporate-Human-Rights-Policy.pdf>

¹⁶ UN General Assembly Resolution 217A(III), 10 December 1948.

¹⁷ UN General Assembly Resolution 2200A (XXI), 16 December 1966, in force 23 March 1976. Ratified by Mauritius on 12 December 1973.

¹⁸ UN Human Rights Council, Report of the independent international fact-finding mission on Myanmar, 18 September 2018, paras. 31-35, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/274/54/PDF/G1827454.pdf?OpenElement>.

¹⁹ *Ibid.*, paras. 20-23.

not. Facebook has been criticised for acting too slowly to address this problem, to which the Myanmar military contributed directly, but the fact that it did take action,²⁰ even if belatedly, directly contradicts the spirit of the claims in the Consultation Paper, namely that social media companies are insensitive to the needs of individual countries.

The paper also significantly distorts the intrusive nature of various international measures to address harmful online content. For example, the German Network Enforcement Act manifestly does not require social media companies to remove illegal content within 24 hours of it being uploaded (paragraph 4.1.1). Instead, the Act requires them to remove “manifestly illegal” content within 24 hours of receiving a complaint about it,²¹ and then gives them seven days, or longer if they refer the matter to binding decision-making by a “recognised self-regulation institution” within seven days.²² Together, these features render the approach of the German Act fundamentally different from the Consultation Paper’s claims about that Act. The Consultation Paper also significantly mischaracterises the EU Regulation on addressing the dissemination of terrorist content online (paragraph 4.4.1). The Regulation provides that takedowns shall occur within one hour of the receipt of an official takedown order, not “within an hour” (with the impression left that this means from the time of uploading, a totally different matter).²³ Furthermore, the Regulation does not necessarily call for fines for social media companies if they do not take the content down, as claimed in the Consultation Paper; instead, EU Member States are left to design their own system for penalties,²⁴ with fines being only mandated for systemic or persistent failures.²⁵

Violations of the Rights to Privacy and Expression

The Core Workings of the Consultation Paper's Proposals

²⁰ Facebook, An Independent Assessment of the Human Rights Impact of Facebook in Myanmar, 5 November 2018, <https://about.fb.com/news/2018/11/myanmar-hria/>; see also The National, “Facebook takes action against Myanmar over Rohingya violence”, 28 August 2018, <https://www.thenationalnews.com/world/asia/facebook-takes-action-against-myanmar-over-rohingya-violence-1.764333>.

²¹ Act to Improve Enforcement of the Law in Social Networks (NetzDG), section 3(2)(2), English translation available at:

https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=AD99C47B2608D12B014859D5FF786F29.2_cid289?__blob=publicationFile&v=2.

²² *Ibid.*, section 3(2)(3).

²³ Regulation of the European Parliament and Council on addressing the dissemination of terrorist content online, adopted on 16 March 2021, Article 3(3), <https://data.consilium.europa.eu/doc/document/ST-14308-2020-REV-1/en/pdf>.

²⁴ *Ibid.*, Articles 18(1)-(2).

²⁵ *Ibid.*, Article 18(3).

The Consultation Paper proposes to intercept all social media traffic travelling to and from Mauritius by creating a proxy server, run by the ICTA, through which all such communications would need to pass (paragraphs 11.1, 11.2.1). However, many social media companies encrypt messages end-to-end, which protects them from being read by parties other than the intended recipient(s). Thus, Facebook encrypts social media traffic so that even if someone manages to intercept, for example, a private message sent between spouses, that person cannot read the message.

Simply requiring communications to pass through a proxy server would not affect any encryption to which they are subject. To break encryption, the Consultation Paper proposes to require every person inside Mauritius who wishes to use social media to install a type of software called a Certification Authority (CA) certificate onto their devices the first time they access a social media website (paragraph 11.3). This certificate would effectively empower the ICTA to impersonate each Mauritian social media user in their interactions with social media websites, thereby activating those websites' decryption systems for the traffic which the ICTA's proxy server has intercepted to and from that user.²⁶

The next step would be for the ICTA to apply "data analysis software" to search all of that decrypted social media traffic for "specific keywords, comments posted, etc" and then correlate it with the relevant IP address (paragraph 11.2.1.d). The Paper also refers to the idea of archiving all of this content (paragraph 11.1) and of responding to complaints (paragraph 11.2.1). For offending content (see below for a more detailed description of this), a range of measures would be taken. It suggests that social media pages which were "incriminated" could be blocked without blocking the entire social media website; that "fake profile" pages could also be blocked and the originators located; and that the individual originators of "offensive comments", for example those posted on a newspaper's social media page, could be identified (and presumably punished), without blocking the newspaper's page. It thus appears that a combination of blocking and other measures is envisaged.

The Consultation Paper does not elaborate in any detail on the specifics of this system, such as what type of data analysis software will be used, whether any human rights safeguards will be applied and how complaints will be processed. It does indicate in a very general way which bodies will be responsible for running the system, which is addressed further below under Independence of Oversight Agencies.

Substantive Violations of the Rights to Expression and Privacy

²⁶ Ish Sookun, "ICT Authority's proposal to monitor the internet, in a nutshell", SysAdmin Journal, 19 April 2021, <https://sysadmin-journal.com/ict-authority-proposal-to-monitor-the-internet-in-a-nutshell/>.

The proposals in the Consultation Paper would violate the rights to freedom of expression and privacy, which are guaranteed to Mauritians by the ICCPR²⁷ and the *African Charter on Human and Peoples' Rights* (ACHPR).²⁸

The freedom of expression as guaranteed under international law, including in Article 19(2) of the ICCPR, is not absolute but any restrictions on this right must meet a three-part test as set out in Article 19(3) of the ICCPR. First, the restriction must be provided by law, which includes a requirement that the law be clear and precise. Second, the restriction must aim to protect one of specific interests listed in Article 19(3), namely the rights or reputations of others, national security, public order, public health or public morals. Third, the restriction must be necessary to protect that interest, which includes a proportionality element.²⁹ Among other things, the UN Human Rights Committee has noted that this means that “restrictions must not be overbroad” and “be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected”.³⁰ The right to privacy, as guaranteed by Article 17 of the ICCPR, is similarly not absolute but interferences must meet the strict standards set out in the ICCPR, in particular that they are not unlawful or arbitrary.

The Consultation Paper suggests that the content that will be targeted by the system will be content that is “harmful and illegal content” (see paragraph 6.3 and 6.8). This, in turn, seems to be drawn from section 18(1)(m) of the ICT Act, which lists as one of the functions of the functions of the ICTA to “take steps to regulate or curtail the harmful and illegal content on the Internet and other information and communication services”.³¹ Some of the key definitions of this sort of content appear to be found in sections 46(ga) and (ha) of the ICT Act, which are specifically quoted in paragraph 6.9 of the Consultation Paper.

Section 46(ga) criminalises using telecommunications equipment to send messages that are “obscene, indecent, abusive, threatening, false or misleading” and which are likely to “cause annoyance, humiliation, inconvenience, distress or anxiety” to any person. Section 46(ha) criminalises the use of information and communication service to impersonate another person in a manner which is likely, again, to cause “annoyance, humiliation, inconvenience, distress or anxiety”.

²⁷ Note 17. Ratified by Mauritius on 12 December 1973.

²⁸ Adopted at Nairobi, Kenya, 26 June 1981, in force 21 October 1986. Ratified by Mauritius on 19 June 1992.

²⁹ UN Human Rights Committee, General Comment No. 34, Article 19: Freedoms of opinion and expression, 12 September 2011, para. 22, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>.

³⁰ *Ibid.*, para. 34.

³¹ See note 3.

These sections are problematical in terms of all three parts of the international test for restrictions on freedom of expression.³² They fail to pass the first part of the test because many of the terms used are too vague to provide sufficient guidance to allow those subject to them to regulate their conduct. In terms of substance, terms such as “indecent”, “abusive” and “misleading” are not defined and could be interpreted to be given a broad range of meanings. They could be deemed to cover anything from a scathing restaurant review to harsh criticism of a politician. Even the term “false” has been held by leading courts around the world, including in Africa, not to be susceptible of clear interpretation. As the Supreme Court of Zimbabwe noted, in striking down a provision which banned the making of a “false statement”:

What is overlooked in the criminalisation of false statements is that language is used in a variety of complex and subtle ways. It is simply not possible to divide statements clearly into categories of fact and opinion.³³

The required results are also manifestly unclear. What, for example, does it mean to cause “annoyance”, “humiliation” or “anxiety” to someone. The wording of section 46(ha), for example, would make criminals of teenagers pretending to be each other and sending prank messages to tease their friends.

These restrictions also do not meet the second part of the test for restrictions since they do not serve to protect one of the legitimate interests listed in Article 19(3) of the ICCPR. While individuals have a right to reputation, they do not have a right not to be annoyed, inconvenienced or even made anxious. If they did, many commonplace social situations, such as getting delayed by traffic, would be illegal. Under international law, it is simply not legitimate to ban speech to avoid these sorts of results. Clearly these results bear no relation to other legitimate interests, such as national security or public order.

Finally, these content restrictions do not meet the third part of the test which, as noted above, requires restrictions to be proportionate and to represent the least intrusive means of achieving an objective. Even if it were permissible to restrict misleading statements to prevent annoyance, which as noted above it is not, this could never meet the standard of proportionality. It is abundantly clear that the harm that would be done to freedom of expression through such a restriction vastly outweighs any social benefit that the restriction might serve, thus resulting in a failure of proportionality.

Worryingly, although it is not clear on this point, the Consultation Paper suggests that there may be a separate category of merely “harmful content” which is not also illegal that the

³² In parallel to making this submission, CLD is releasing an Analysis of the ICT Act that analyses these and other problematic provisions.

³³ *Chavunduka & Choto v. Minister of Home Affairs & Attorney General*, 22 May 2000, Judgement No. S.C. 36/2000, Civil Application No. 156/99.

system would seek to capture. Although most of the references to “harmful content” in the Consultation Paper are linked to “illegal content” using “and” as a conjunction (as in “harmful and illegal content”), paragraph 6.8 suggests that this is a separate category of content which is “more subjective” and in relation to which the ICTA is not “presently vested” with investigatory powers. While it is not stated as such, the implication is that the new regime might address this apparent shortcoming.

The usage of data analysis software to identify harmful and illegal content, as proposed in the Consultation Paper, could also potentially implicate freedom of expression. So far, the capacity of automated systems to detect or identify illegal content reliably is limited in several ways, for example due to their limitations in recognising irony, comedy and certain forms of critical analysis. As such, it is only where the use of automated systems is followed up by human review, as always subject to appropriate due process and appeal rights, that they can meet the standards required under international law for imposing restrictions on freedom of expression.³⁴ The Consultation Paper does not elaborate on how this system will work but, if it does not involve expert and independent human review of automated decisions, it could have a significant adverse impact on freedom of expression by singling out perfectly legal content for sanctioning measures.

The right to use encryption tools and to practise anonymity have been recognised as being foundational to protecting the rights to both freedom of expression and privacy in the digital space. As the UN Special Rapporteur on freedom of expression has noted: “Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.”³⁵ Similarly, all four special international mandates on freedom of expression have recognised that, as part of their obligations to create an enabling environment for freedom of expression, States should: “Refrain from arbitrary or unlawful restrictions on the use of encryption and anonymity technologies”.³⁶

The Consultation Paper’s proposals to breach encryption violate both the right to freedom of expression and the right to privacy. The indiscriminate, untargeted nature of the proposals to breach encryption mean that they cannot pass the necessity part of the test for

³⁴ See, for example, the Council of Europe’s Committee of experts on internet intermediaries’ (MSI-NET) *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, March 2018, pp. 16-22, <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

³⁵ Report to the Human Rights Council of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, para. 16, https://www.ohchr.org/EN/HRbodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

³⁶ Special international mandates on freedom of expression at the UN, OSCE, OAS and ACHPR, Joint Declaration on Challenges to Freedom of Expression in the Next Decade, 10 July 2019, para. 1g, https://www.law-democracy.org/live/wp-content/uploads/2019/07/Mandates.decl_.2019.20th.English.pdf.

restrictions on freedom of expression or the requirement that interferences with privacy not be arbitrary.

A proportionality analysis in the context of mass archiving of content, as seems to be proposed in the Consultation Paper (see paragraph 11.1), also requires State actors to consider whether their interference with these protections might enable exploitation by malign external actors such as terrorists or extremists.³⁷ The Consultation Paper's proposals envision all social media traffic being copied and stored on the ICTA's proxy server (paragraph 11.1). While that data would be protected by Mauritius' Data Protection Act 2017 (paragraph 8.4), the severe consequences if the data of every social media user in Mauritius nonetheless become exploited make the proposals even more disproportionate to their ill-defined aims.

Violations Due to the Means of Implementation and Sanctions

It is not just the substance of the restrictions on freedom of expression and privacy in the Consultation Paper's proposals that are problematical. The manner of implementation of those substantive restrictions also fails to pass muster according to the tests under international law for restricting these rights. In particular, the proposed mass surveillance of communications violate both of these rights. Looked at from the perspective of privacy, the UN Human Rights Committee has explained that the proscription on arbitrary interferences is intended to ensure that even "interference provided for by law ... should be, in any event, reasonable in the particular circumstances."³⁸ The vast overbreadth of the programme of mass surveillance following breach of encryption in the Consultation Paper's proposals mean that it cannot be reasonable based on the circumstances. The UN Human Rights Committee has made it clear that where restrictions on privacy are allowed by law, they must be authorised on a "case-by-case basis",³⁹ which rules out mass surveillance. The UN Human Rights Committee has also called for prohibitions on general measures of surveillance and interception of communications, stating that these, "should be prohibited."⁴⁰ Similarly, as the UN Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion has pointed out, "measures that impose

³⁷ See note 35, para. 35.

³⁸ General Comment No. 16: Article 17 (Right to Privacy), 8 April 1988, para. 4, http://ccprcentre.org/page/view/general_comments/27798#:~:text=Article%2017%20provides%20for%20the,on%20his%20honour%20and%20reputation.

³⁹ *Ibid.*, para. 8.

⁴⁰ *Ibid.*

generally applicable restrictions on massive numbers of persons, without a case-by-case assessment, would almost certainly fail to satisfy proportionality.”⁴¹

Under international law it is not only the substance and means of implementation of restrictions on freedom of expression that must be proportionate but also any sanctions or measures that are applied following the identification of illegal material. For its part, section 47 of the ICT Act provides for a fine of up to MUR1,000,000 (approximately USD 24,000) and (not “and/or”) up to ten years’ imprisonment (“penal servitude”) for breach of its provisions, as well as the forfeiture of any equipment used and the loss of any licence held.⁴² For their part, the Consultation Paper’s proposals call for the content-adjudication agency to refer harmful and illegal content to the ICTA for blocking (paragraph 8.3.3) and to the police, presumably for criminal investigation purposes (paragraph 8.3.4). Other parts of the Consultation Paper suggest that both blocking and criminal sanctions will be applied to offending content (see, for example, paragraph 11.2.1).

Section 47 is a generic penalty provision which covers all of the offences set out in the ICT Act, some of which, such as committing fraud or destroying property, are potentially fairly serious and might warrant imprisonment. However, serious fines and certainly imprisonment would only in the very most rare and extreme cases be warranted for any content that might in practice be spread over social media. Even where some sort of sanction might be warranted for content shared over social media, such as for breach of reputation or more serious invasions of privacy, a warning or minor damage award would normally be the most serious sanction that could be justified given the right to freedom of expression.

As for the blocking measures that appear to be routinely envisaged for harmful and illegal content according to the Consultation Paper’s proposals, these will also rarely be legitimate due to their disproportionate nature. Rather than blocking a user’s account or page, which paragraph 11.1(a) envisages as being preferable to blocking the whole social media website, it would normally be sufficient to request the user or the social media platform administrator to takedown the specific offending content. Where this failed to produce results, other measures could potentially be considered. Paragraph 8.3.3 does appear to envisage contacting the social media platform administrator, although it is not clear how long that approach will be given to resolve the problem before the matter is referred to the ICTA for more muscular measures.

Independence of Oversight Agencies

⁴¹ See note 35, para. 43.

⁴² See note 3.

Under international law, any bodies which exercise regulatory powers over freedom of expression need to be independent. For example, in their 2003 Joint Declaration, the special international mandates on freedom of expression at the UN, OAS and OSCE stated:

All public authorities which exercise formal regulatory powers over the media should be protected against interference, particularly of a political or economic nature, including by an appointments process for members which is transparent, allows for public input and is not controlled by any particular political party.⁴³

Although this has historically most commonly been expressed in relation to media regulators, given that these were the bodies one normally found in different countries with such regulatory powers, the same rationale applies to any regulation of social media as well. And that rationale is quite simple, namely that if government exerts control or even significant influence over such regulatory powers, decisions will be made on political rather than objective grounds, undermining freedom of expression.

It is clear that the proposed mass interception, storage, surveillance and applications of restrictions to all social media traffic originating from Mauritius creates enormous potential for abuse if the oversight of the system was not robustly independent of government and political actors. To name just two possibilities, political actors could use the system to identify and persecute political opponents or selectively enforce content-blocking powers to suppress negative stories about incompetence or worse on the part of politicians or officials. The importance of protecting the operation of this system against political interference so as to limit human rights risks is therefore clear.

The Consultation Paper envisages two key bodies playing a role in enforcing the new system, namely a National Digital Ethics Committee (NDEC), a key role of which will be to decide whether content is harmful and illegal content, and a Technical Enforcement Unit, the key role of which will be “to enforce the technical enforcement measures as directed by the NDEC” (paragraph 7.2; see also paragraph 8.3.2).

The drafters of the Consultation Paper were obviously aware of the idea of independent regulation, stating that the chair and other members shall be “independent, and persons of high calibre and good repute” (paragraph 9.1). While this is an encouraging start, true structural independence would require legal protections such as an appointment process that is designed to prevent political interference given the social and political environment in Mauritius, fixed-term tenure and protections against removal of members with sufficient due process safeguards, and a system for allocating the budget and remunerating members

⁴³ 18 December 2003, <http://www.osce.org/fom/66176>. The special international mandates, now four with the addition of the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, have adopted a Joint Declaration on a freedom of expression theme every year since 1999.

which is similarly protected against political interference. Given the scant details in the Consultation Paper on this, it is not possible to assess at this point whether there are protections for independence and how robust they are.

However, the proposed Technical Enforcement Unit, which will run the very sensitive so-called “technical toolset” that lies at the heart of the whole system, will be housed within the ICTA (paragraph 10.1). As such, the Technical Enforcement Unit will be directly responsible for executing the mass surveillance, encryption-breaking and content restriction measures. Given that the latter is not remotely either formally or structurally independent, the Unit also cannot hope to achieve this status. The ICTA is not independent because, among other things, appointments to its governing board are almost entirely controlled by the government (section 5(3) of the ICT Act), with several members directly representing ministries and only the chair being chosen following any form of consultation, in that case with the leader of the opposition. There are also vague and somewhat arbitrary grounds for removal of members (see sections 7(1)(c) and (d) of the ICT Act), presumably exercised again by the government, and members hold office on such terms and conditions of service as the prime minister may determine, rather than fixed terms and tenure (section 5(4)(b) of the ICT Act). Furthermore, the minister responsible for ICT can issue general directions to the board which it is required to follow (section 19 of the ICT Act).

The Proposals May Not Deliver the Desired Results

The intrusiveness of the proposals in the Consultation Paper may well produce negative reactions from major social media platforms like Facebook and Twitter. There is a risk that they might restrict or simply close off the availability of their services in Mauritius rather than permit them to be associated with the massive freedom of expression and privacy breaches, not to mention information security risks, which the proposals entail.

There is also a growing range of digital tools that can be used to thwart the Consultation Paper’s proposals. For example, the use of a Virtual Private Network (VPN) could circumvent the whole scheme. VPNs effectively allow users to adopt an IP address that is external to Mauritius or provide IP trackers with a false address, thereby evading the ICTA’s interception and impersonation process. China, the world’s most sophisticated practitioner of technological authoritarianism, has only relatively recently managed to plug some of the vast holes in its Great Firewall that are posed by VPNs and it is still working to block the other leaks.⁴⁴ We cannot assess the technical sophistication available to Mauritius and the ICTA, but it seems unlikely that it would be able to operate at the level of China. To

⁴⁴ Frank Chen, “VPNs escape Beijing’s iron grip on web, for now”, Asia Times, 4 March 2020, <https://asiatimes.com/2020/03/vpns-escape-beijings-iron-grip-on-web-for-now/>.

be clear, CLD is not suggesting that the ICTA should develop the technological capacity to be able to run the proposed system. Rather, it is our position that the benefits of the proposals are likely to be seriously qualified, and that sophisticated users, who are also likely to be those posing greater risks of actual harm, are likely to be able to get around it.

Finally, a number of the harms listed in the Consultation Paper would fall entirely or almost entirely outside of the scope of this system. Thus, hacking, by far the most prevalent type of problem listed in the table found at paragraph 6.1 of the Paper, would be almost or entirely untouched by these measures. It is unclear how effective the proposed system would be against identity theft, another common problem listed in that table, and many of the other problems are committed via multiple means of communications and not just through social media.

Alternatives to the Extreme Solution Proposed

The Consultation Paper claims that the inability of Mauritius to enforce legal orders on social media companies, given their lack of physical presence in the country, makes the proposed extreme measures “the only logical and practical solution” available to it (paragraph 6.3). This claim is suspect.

In fact, there are many logical and more practical options available to the government other than the highly intrusive measures it is proposing. To start with, the government should consider using existing remedies such as working more closely with social media companies. As pointed out in the first section of this Note, it is not true that these companies are completely indifferent to the views of governments and the needs of different countries. CLD urges the Mauritian government to release, in the interest of transparency, details of any attempts they have made to negotiate with social media companies to address in a cooperative fashion the ills the Consultation Paper discusses. If no such overtures have been meaningfully pursued, then less extreme measures have clearly not been exhausted.

Another option would be for the Mauritian government to build the capacity of its citizens by putting in place proper media and information literacy (MIL) measures to combat disinformation and other forms of problematical content. UNESCO has been calling for the use of MIL to combat disinformation, and their website contains a list of resources that could serve as a starting point in this area.⁴⁵ For example, the Belgrade Recommendations

⁴⁵ UNESCO, Media and Information Literacy – Resources, <https://en.unesco.org/themes/media-and-information-literacy/resources>.

on Draft Global Standards for Media and Informational Literacy Curricula Guidelines⁴⁶ provide a useful roadmap for how a government could effectively implement MIL training.

There may also be more to be done in terms of building effective capacity to combat cybercrimes, which the proposals in the Consultation Paper will only very partially address. There are various publicly available resources on how to build capacity to fight cybercrime, such as the World Bank's toolkit on *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*.⁴⁷

The measures discussed above constitute more effective and sustainable, not to mention far more human rights compliant, solutions to both more serious criminal harms being perpetrated through digital communications and the less extreme but still potentially overall negative impact of certain forms of communication over social media. These measures should, therefore, be applied before resorting to more intrusive measures.

Recommendations

- The Mauritian government should abandon entirely the proposals in the Consultation Paper based on a system of mass surveillance, breach of encryption and vague, overbroad content restrictions.
- The Mauritian government should ensure that any new or existing regulatory bodies that have the power to regulate freedom of expression benefit from both formal and structural protections against political or commercial interference.
- The Mauritian government should release details of any attempts it has made to cooperate with social media companies. Meaningfully cooperate with social media companies, if not yet attempted, should be pursued with the aim of addressing some of the harms cited in the Consultation Paper.
- The Mauritian government should put in place an effective system to build the capacity of its citizens in terms of media and information literacy and the ability of relevant institutions to fight cybercrime.

⁴⁶ 13 September 2019,

https://en.unesco.org/sites/default/files/belgrade_recommendations_on_draft_global_standards_for_mil_curricula_guidelines_12_november.pdf.

⁴⁷ World Bank, *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*, August 2017, <https://openknowledge.worldbank.org/handle/10986/30306?locale-attribute=fr>.

