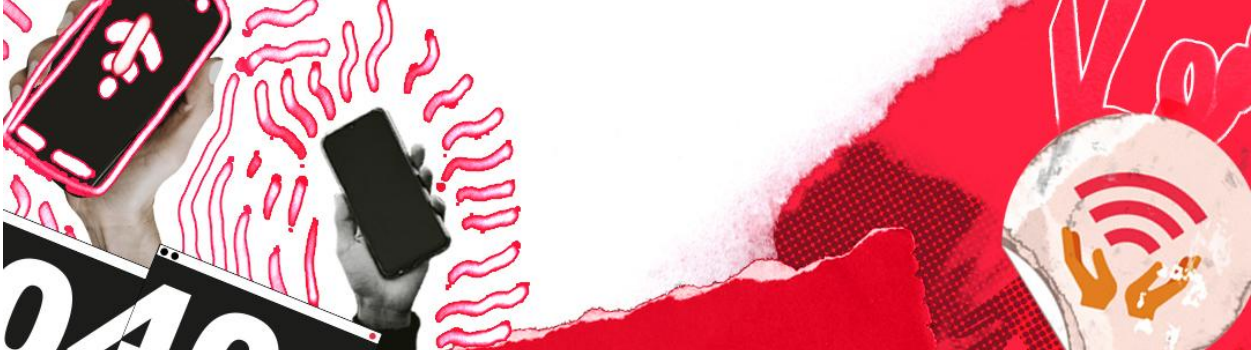


May 12, 2021

Joint civil society statement in response to the *Information & Telecommunications Authority Consultation paper on proposed amendments to the ICT Act for regulating the use and addressing the abuse and misuse of Social Media in Mauritius* dated April 14, 2021

Attn:
Information & Communication Technologies Authority (ICTA) of Mauritius
Government of the Republic of Mauritius

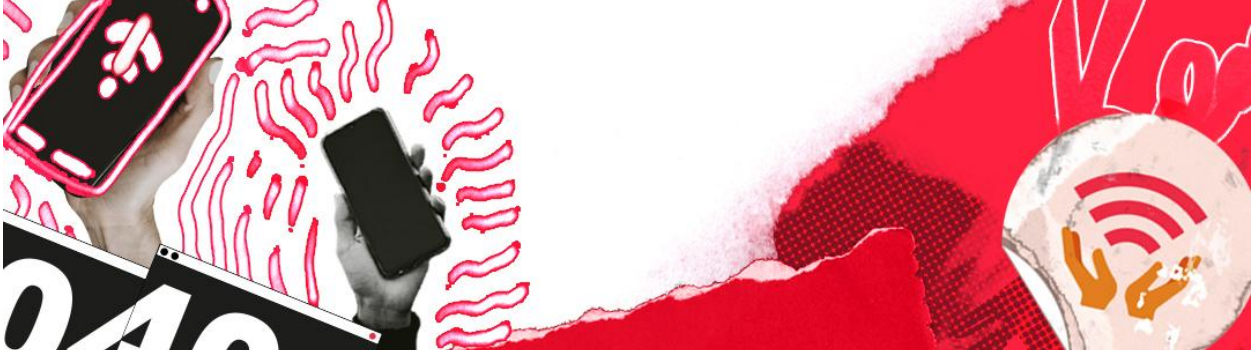
We are writing, as a group of international allies and advocates for freedom of expression including press freedom and human rights, to respond to the consultation paper issued on 14 April 2021 by the Information & Communication Technologies Authority (ICTA) of Mauritius, laying out a set of proposed amendments to the existing Information and Communication Technologies Act. We believe that the proposed amendments present a threat to human rights—specifically, the rights to privacy and freedom of expression including press freedom— of the people of Mauritius. Mauritius is widely viewed as a leading democracy in the African Union[1], and boasts a strong economy,[2] but this consultation paper represents a worrying trend in the country, coming as it does on the heels of 2018 revisions to the ICT Act which criminalized additional categories of online speech.[3] The proposed amendments to the ICT law are radically disproportionate to their stated aims of countering offensive speech on social media, and would set a dangerous precedent, allowing state surveillance of the lawful conduct of private citizens, and undermine the digital security of the internet as a whole by attacking encryption. It is particularly worrying that the loosely worded or vague definitions in the proposal fare even worse than the Computer Misuse & Cybercrime Act requirements on investigations & procedures.

---

[1] Intercontinental Trust, "Democracy Index 2019: Mauritius a "Full Democracy" and ranks 1st in Africa, 18th worldwide" (March 26, 2020). https://intercontinentaltrust.com/latest-news/democracy-index-2019-mauritius-a-full-democracy-and-ranks-1st-in-africa-18th-worldwide

[2] Klaus Schwab (Ed.), "The Global Competitiveness Report 2017-2018" (World Economic Forum). http://www3.weforum.org/docs/GCR2017-2018/05FullReport/TheGlobalCompetitivenessReport2017%E2%80%932018.pdf

[3] Freedom House, "Mauritius: Freedom in the World 2020 Country Report" (February 28, 2020). https://freedomhouse.org/country/mauritius/freedom-world/2020



May 12, 2021

In brief, the Mauritian regulator proposes to require the decryption of all web traffic deemed to be "social media," by intervening in the issuance of security certificates for HTTPS traffic, which would then be routed through government-controlled proxy servers.[4] A new administrative body, the "National Digital Ethics Committee," would be empowered to make determinations about what content was considered harmful, and such content would then be blocked. This proposed regulatory framework suffers from fatal shortcomings under international human rights standards: firstly, administrative censorship generating chilling effects on speech and secondly, disabling of encryption, crucial for digital security.

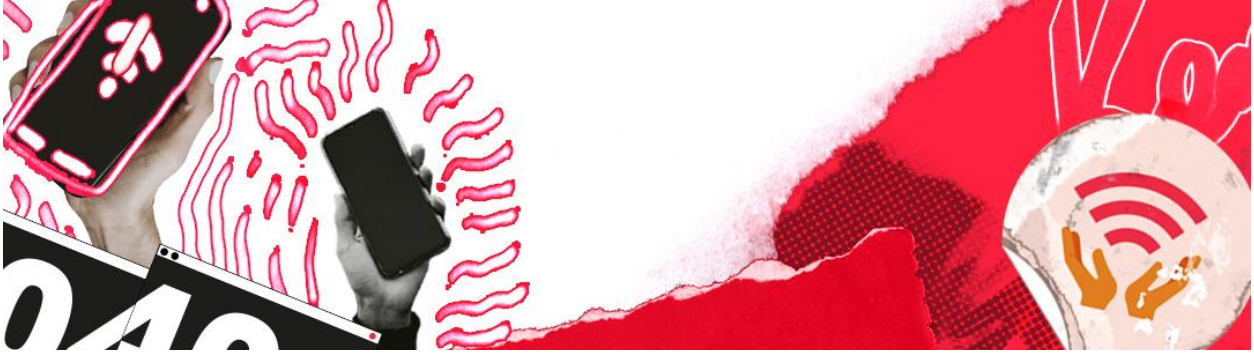
The broad discretion and power conferred to the National Digital Ethics Committee poses significant threats to freedom of expression, privacy, and security. For instance, the new National Digital Ethics Committee would be tasked with identifying "illegal and harmful contents." However, this phrase is not further defined, leaving the Committee with an unacceptable degree of discretion. Although the consultation paper points to French and German policies as examples, the proposed framework is nothing like them: the German NetzDG law is only applicable to speech that violates an enumerated list of Criminal Code provisions, and the French Avia law is similarly specific to ten or so categories of speech, all of them commonly recognized as harmful speech around the world.

Moreover human rights and press freedom organisations in France and Germany have criticized the two laws for not being consistent with international standards.

We are concerned that the proposed provision fails to meet the level of clarity and precision required by Article 19(3) of the ICCPR for restrictions on freedom of expression. To satisfy the requirements of legality, restrictions must additionally be sufficiently clear, accessible and predictable (CCPR/C/GC/34). The wording of the proposed statute does not meet the level of clarity and predictability as required by international human rights law and such ambiguity may confer excessive discretion on the proposed regulatory body and contribute to a chilling effect on the exercise of freedom of expression in digital space.

As currently worded, the National Digital Ethics Committee's decision would be final and implemented by a Technical Enforcement Unit, which would operate the proxy servers. The expansive discretion given to the National Digital Ethics Committee, combined with the opacity of the procedure and the lack of clarity around the standards to define content subject to censorship, appears particularly

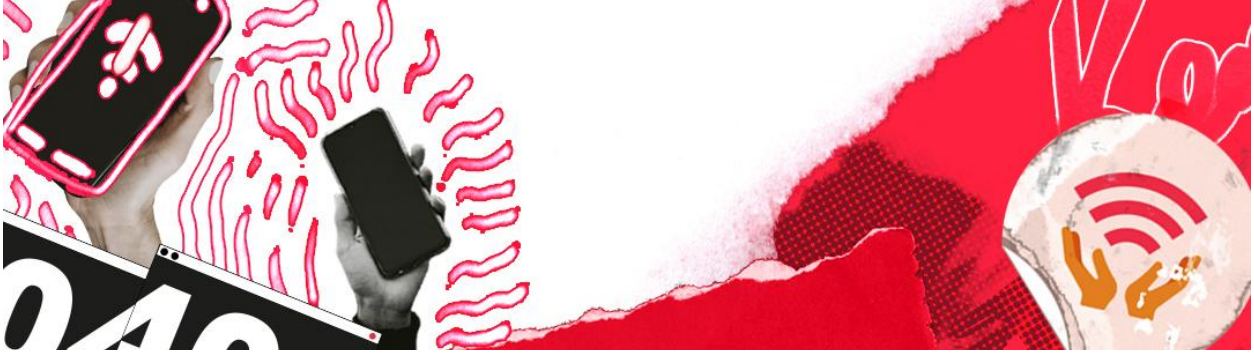
[4] Ish Sookun, "ICT Authority's proposal to monitor the Internet, in a nutshell" (April 19, 2021). https://sysadmin-journal.com/ict-authority-proposal-to-monitor-the-internet-in-a-nutshell/



problematic given extremely limited opportunities for review or appeal of removals. The lack of independent and external review or oversight of removal orders reinforces the unchecked discretion of government authorities and raises concerns of due process. **Consistent with international norms advanced by the Special Procedures of the UN Human Rights Council and the Manila Principles for Intermediary Liability, among other expert bodies, we urge the government to categorically reject a model of regulation "where government agencies, rather than judicial authorities, become the arbiters of lawful expression." (A/HRC/38/35).**[5]

It is important to explain why administrative censorship should be avoided at all costs. Firstly, an administrative body such as the National Digital Ethics Committee, by definition, does not and should not have the final authority because their decisions are always subject to the risk of reversal as the result of subsequent judicial review.[6] The fact that one's speech can be censored by an administrative body without judicial supervision naturally causes a chilling effect on the supposed speaker because subsequent judicial review is time-consuming and cost prohibitive.[7] Secondly, administrative bodies may show bias in favor of the incumbent government in disputes concerning the executive and legislative branches themselves, much more so than the judiciary.[8] In spite of the consultation paper's assertion that the proposed National Digital Ethics Committee would be "independent," there are no procedural guarantees to that effect. Thirdly, administrative bodies usually have the ability to retaliate against the speakers seeking reversal of censorship decisions through other means such as industrial subsidies or licensing schemes through their broader executive powers.[9] For the foregoing reasons, courts in other jurisdictions such as France and Philippines have struck down similar unrestricted

[5] David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/38/35" (April 6, 2018). https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement, pg. 20.
[6] Martin H. Redish, "The Proper Role of the Prior Restraint Doctrine in First Amendment Theory", 70 Va. L. Rev. 53, 58 (1984).
[7] "The Chilling Effect in Constitutional Law", 69 Columbia Law Review 808 (1969).
[8] William T. Mayton, "Toward a Theory of First Amendment Process: Injunctions of Speech, Subsequent Punishment, and the Costs of the Prior Restraint Doctrine", 67 Cornell L. Rev. 245, 250 (1982).
[9] Henry P. Monaghan, "First Amendment "Due Process", 83 Harv. L. Rev. 518, 522-23 (1970).



delegations of censorship authority to administrative bodies,[10] and the number of democracies around the world that endow administrative bodies with any censorship authority is vanishingly small.[11]

Secondly, the mandated decryption of all social media traffic is an unprecedented and deeply distressing restriction on privacy, a freedom guaranteed by the ICCPR in Article 17, whether it is for "inspection" by the government or for any other purpose. HTTPS has provided security for internet users around the world. Not only the Mauritian people, but others globally who are in contact with Mauritian citizens, have the right to communicate privately, and such privacy supports people's freedom of speech. Encryption and anonymization technologies establish a "zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks" (A/HRC/29/32). As such, any restrictions on these technologies must meet the well-known three-part test established under Article 19(3) of the International Covenant on Civil and Political Rights: they must be provided for by law, imposed on legitimate grounds, and both necessary and proportionate. As a recent UN Special Rapporteur wrote, "States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows."[12] The proposed framework would undo all of the rights-protective benefits provided by encryption of web traffic, and thereby would unduly interfere with freedom of expression and privacy and would pose a danger to the confidentiality of journalists' sources. It is telling that the only government that has proposed a similar (though in fact, more limited) mechanism is Kazakhstan, which halted the deployment of the program in 2019 after public outcry — including global concern that it would undermine the digital security of internet communications and represent a tremendous threat to cybersecurity.[13] It is even more troubling that the Mauritian proposal would enable the

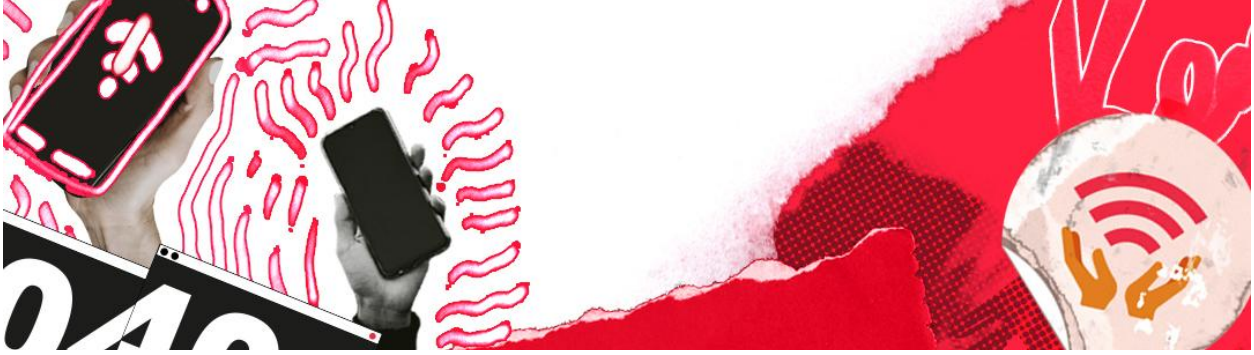
---

[10] Conseil constitutionnel, "Decision n° 2009-580 of June 10th 2009" (June 10, 2009). http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf; Conseil constitutionnel, "Décision n° 2020-801 DC du 18 juin 2020" (June 18, 2020). https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm; Rappler, "FULL TEXT: Cybercrime law constitutional – Supreme Court". http://www.rappler.com/nation/special-coverage/cybercrime-law/51197-full-text-supreme-court-decision-cybercrime-law

[11] These include Korea (see Kyung Sin Park, "Administrative Internet Censorship by Korea Communication Standards Commission" (December 24, 2014), Soongsil Law Review, Vol. 33, January 2015, pp. 91-115. https://ssrn.com/abstract=2748307) and Turkey (see http://eng.btk.gov.tr/).

[12] David Kaye, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/29/32)" (May 22, 2015). https://freedex.org/encryption-and-anonymity/, pg. 20.

[13] Freedom House, "Kazakhstan: Freedom on the Net 2020 Country Report" (October 13, 2020). https://freedomhouse.org/country/kazakhstan/freedom-net/2020



collection and unprotected local storage of a vast amount of user data without any specific timeline for expungement.

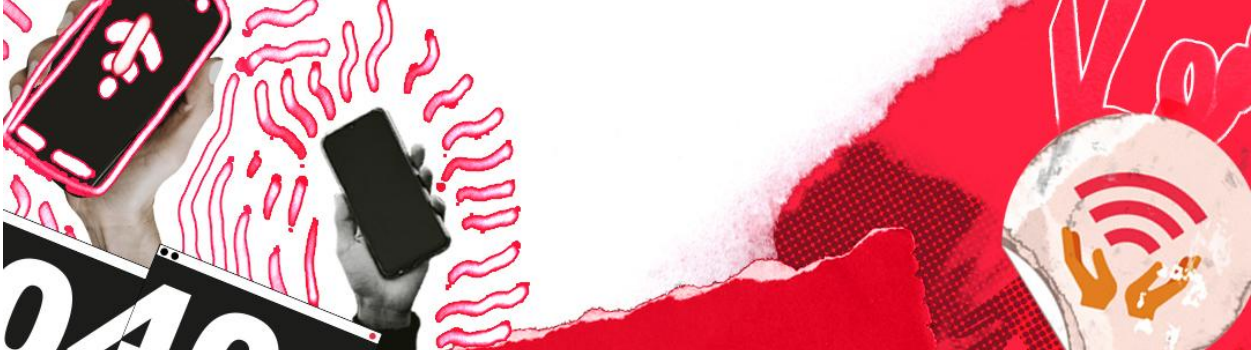
As a leading regional democracy, Mauritius should consider the fact that governments around the world have encouraged the use of HTTPS to create an environment free of hacking and surveillance.[14] It goes without saying that none of the laws referred to in the consultation paper require the indiscriminate decryption of data flowing from social media — which unfortunately is the thrust of the proposal in Mauritius.

The proposed mandatory decryption has human rights consequences beyond its text: the Consultation Paper proposes that users who do not consent to their social media traffic being directed to a government platform, then decrypted and archived, will be denied access to the online service provider. **This attempt is tantamount to access blocking and raises fundamental questions about Internet access. It would be a regressive measure at a time when the international community seeks to promote access worldwide and to act to reduce the digital divide.**

Furthermore, the technical toolset requiring interception, decryption and archiving of social media traffic, no matter how it is implemented, will break end-to-end encryption. The fundamental tenet of end-to-end encryption is that no one other than the sender and the recipient, including the service provider, can decrypt the relevant data. The proposed technical toolset will make it impossible for any social media platform to offer end-to-end encryption in Mauritius, enabling "monster-in-the-middle" attacks. This is extremely problematic for digital rights and internet freedom for all. **Breaking end-to-end encryption is a threat to cybersecurity and information security, which could expose more data than the proposal contemplates and put the safety of all stakeholders at risk.** It must therefore clear the necessity and proportionality test that is recognized internationally as the standard for such measures, and the proposed law does not.

The proposed law would undoubtedly reverse the gains that have been made by the government of Mauritius in the area of human rights. We call on the government and ICTA in particular to retract the consultation paper, which proposes radically disproportionate measures to counter offensive speech on social media and presents a threat to human rights--specifically, the rights to privacy and free expression including press freedom. If it is sincere in its desire to uphold human rights and democratic

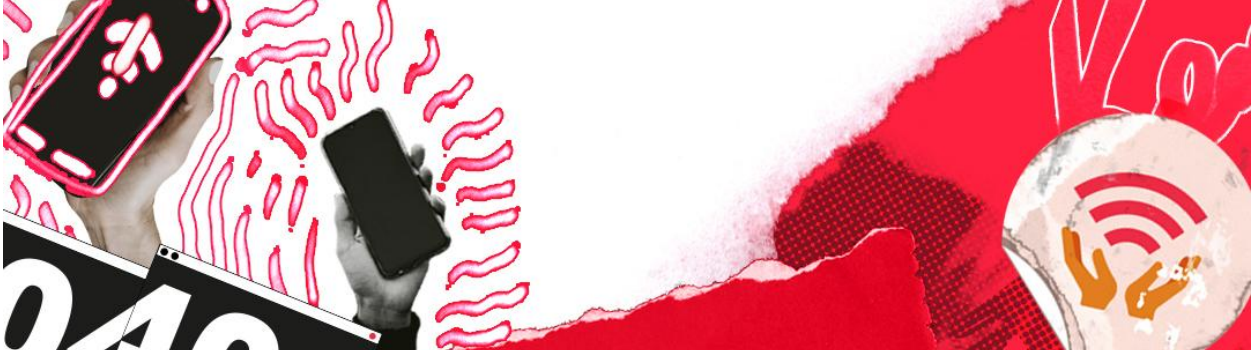
[14] See, e.g., "Resolution adopted by the Human Rights Council on 23 March 2017 A/HRC/RES/34/7" (March 23, 2017).
https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2FRES%2F34%2F7&Language=E&DeviceType=Desktop



principles, the government can explore more proportionate and rights-protective measures, appropriate to the context of a free society, for the regulation of illegal conduct on social media.

ORGANIZATIONS

Access Now
Advocacy Initiative for Development (AID)
African Declaration on Internet Rights and Freedoms Coalition
African Freedom of Expression Exchange (AFEX)
Africa Open Data and Internet Research Foundation (AODIRF)
AfricTivistes
AI for the People
Bareedo Platform Somalia
Change Tanzania movement
Center for Democracy & Technology
Centre for Multilateral Affairs (CfMA)
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Committee to Protect Journalists (CPJ)
Computing and Information Association
Electronic Frontier Foundation
FairSquare Projects
Fundación InternetBolivia.org
Gambia Press Union (GPU)
Global Voices
INSM Network - Iraq
Internet Without Borders
Last Mile4D
Media Foundation for West Africa (MFWA)
OpenNet Africa
Open Net Association
Organization of the Justice Campaign
Reporters Without Borders (RSF)
SMEX
SOAP
Ubunteam
Unwanted Witness
Wikimédia France
Women of Uganda Network (WOUGNET)
Women ICT Advocacy Group (WIAG)
Aditya Sharma, Commonwealth Human Rights Initiative
Andrea NGOMBET, Sassoufit Collective
Ekai Nabenyo, Paradigm Initiative
Jessica Fjeld, Harvard Law School / Berkman Klein Center for Internet & Society
Jenny Korn, Harvard Law School / Berkman Klein Center for Internet & Society
Jonnie Penn, Berkman Klein Center for Internet & Society at Harvard University
Kyung Sin Park, Korea University School of Law
Marcus KISSA, Sassoufit Collective
Mason Kortz, Harvard Law School / Berkman Klein Center for Internet & Society
Mikhail Klimarev, Internet Protection Society (Russia)
Nani Jansen Reventlow, Digital Freedom Fund
Paola Ricaurte, Berkman Klein Center for Internet & Society at Harvard University/Tierra Común
Rapudo Hawi, Kijiji Yeetu, Kenya
Ram Shankar Siva Kumar, Microsoft and Harvard University



May 12, 2021

Rebecca Tabasky, Berkman Klein Center for Internet & Society at Harvard University
Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

Shreya Tewari, Harvard Law School / Berkman Klein Center for Internet & Society
Thorsten Busch, University of St. Gallen, Switzerland

For More Information, please contact: press@accessnow.org