May 28, 2021

Dear H.E. Johnny G. Plate,
Minister of Communication and Information Technology
Ministry of Communication and Information Technology, Indonesia

We, the undersigned, urge you to repeal Ministerial Regulation 5/2020 (MR5) that is deeply problematic, granting government authorities overly broad powers to regulate online content, access user data, and penalize companies that fail to comply.

MR5 governs all private "electronic systems operators" that are accessible in Indonesia, broadly defined to include social media and other content-sharing platforms, digital marketplaces, search engines, financial services, data processing services, and communications services providing messaging, video calls, or games. This new regulation will affect national and regional digital services and platforms, as well as multinational companies like Google, Facebook, Twitter, and TikTok.

These companies are required to "ensure" that their platform does not contain or facilitate the distribution of "prohibited content," which implies that they have an obligation to monitor content. Failure to do so can lead to blocking of the entire platform. This requirement for companies to proactively monitor or filter content is both inconsistent with the right to privacy and likely to amount to prepublication censorship.

The regulation's definition of prohibited content is extremely broad, including not only content in violation of Indonesia's already overly broad laws restricting speech, but also any material "causing public unrest or public disorder" or information on how to provide access to, or actually providing access to, prohibited material. The latter includes Virtual Private Networks (VPNs), which allow a user to access blocked content and are routinely used by businesses and individuals to ensure privacy for lawful activities.

For "urgent" requests, MR5 requires the company to take down content within four hours. For all other prohibited content, they must do so within 24 hours of being notified by the Ministry. If they fail to do so, regulators can block the service or, in the case of service providers that facilitate user-generated content, impose substantial fines.

MR5 obliges every "Private Electronic System Operator" (Private ESO) to register and obtain an ID certificate issued by the Ministry before people in Indonesia start accessing its services or content.

Previously registration must take place by May 24th, 2021, but later was postponed based on press conference held by Samuel Pangerapan as General Director APTIKA (Directorate of Application and Informatics) of Indonesia MICT to 6 months until the Single Sign-On (SSO) is ready to be implemented.

Under MR5, Kominfo will sanction non-registrants by blocking their services. Those Private ESOs who decide to register must provide information granting access to their "system" and data to ensure effectiveness in the "monitoring and law enforcement process." If a registered Private ESO disobeyed the MR5 requirements, for example, by failing to provide "direct ac-

cess" to their systems (Article 7 (c)), it can be punished in various ways, ranging from a first warning, to temporary blocking, to full blocking and a final revocation of its registration.

Based on our analysis, MR5 does not comply with standards, legal theory or principles, but also does not uphold freedom of expression and other human rights.

1. The substance of MR5 includes the regulation of digital rights, including restrictions. Considering the right to privacy, it is clear that MR5 exceeds the limits given in Law 12/2011, because it is limited to the framework of "administering certain functions in the government." MR5 therefore has the potential to violate freedom of expression and other human rights.

2. The provisions in MR5 are potentially contrary to Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR); especially the provisions enabling authorities to obtain personal data from Private ESOs. These concerns are compounded by the absence of independent supervision in obtaining access to personal data, and the fact that in practice, personal data is often misused, especially by law enforcement officials.

3. The three-part test has not been strictly regulated in the legal mechanism in MR5, so practically, this arrangement opens up space for violations of human rights, particularly the right to privacy.

4. In MR5, the term "Access Termination" , interpreted as meaning both blocking access to internet and takedown of an account or a social media post, is used 65 times. This has the potential to limit rights and freedoms, and is very likely to interfere with the interests of Private ESOs. Further, the standard of limitation for the termination of access to internet, is not clearly stipulated within MR5, leaving the powers to terminate access open to abuse and disproportionate application. The failure to include an adequate complaints mechanism further compounds concerns that termination of access will be utilised by authorities arbitrarily and excessively.

5. The phrase "prohibited" in Article 9 paragraphs (3) and (4) actually has a very wide range and its interpretation opens up space for debate, especially if there is a conflict of interest of State Institutions or law enforcement officials. For example, what is meant by "public disturbance", what is the standard or measure, who has the authority to determine it, and what if the public feels that it is not part of what is called "disturbing the society"?

6. With regard to Chapter IV, Article 14, regarding requests for termination of access, it is necessary to consider the restriction standards stipulated in Article 19 paragraph (3) of the ICCPR, including considerations of the Human Rights Committee's General Comment No. 34.

7. MR5 requires Private ESOs, including social media platforms and other online-based service providers to comply with domestic jurisdiction, both for content and the use of content in daily practices.. The legal framework for such obligations weakens the protection of all social media platforms, applications, and other online service providers, especially to accept domestic jurisdiction over user data content and policies and practices. Such a legal framework becomes a repressive instrument that would contradict or even violate human rights.

We call on you to immediately repeal MR5.

Regards,

- Access Now (International)
- Amnesty International Indonesia (Indonesia)
- Alliance of Independent Journalists (Indonesia)
- ARTICLE 19
- Digital Reach (Thailand)
- Electronic Frontier Foundation (International)
- EngageMedia (Australia)
- ELSAM (Indonesia)
- Free Expression Myanmar (Myanmar)
- Foundation for Media Alternatives (Philippines)
- Greenpeace Indonesia (Indonesia)
- Human Rights Watch (International)
- Indonesia Corruption Watch (Indonesia)
- Indonesia Legal Aid Foundation (Indonesia)
- Institute for Criminal Justice Reform (Indonesia)
- Komite Perlindungan Jurnalis dan Kebebasan Berekspresi (Indonesia)
- LBH Jakarta (Indonesia)
- LBH Pers Jakarta (Indonesia)
- Manushya Foundation (Thailand)
- Open Net Association (South Korea)
- Oxen Privacy Tech Foundation (OPTF) (Australia)
- Perkumpulan Lintas Feminis Jakarta (Indonesia)
- Southeast Asia Freedom of Expression Network (SAFEnet) (Indonesia)
- TAPOL (United Kingdom)
- Unit Kajian Gender dan Seksualitas LPPSP FISIP UI (Indonesia)