

**Asia Internet Coalition (AIC) Industry Submission on Electronic Information and
Transactions Law (ITE Law) Amendment, Indonesia**

30 December 2023

Minister Budi Arie Setiadi,
Minister of Communications and Informatics
Ministry of Communications and Informatics (KOMINFO),
Jl. Medan Merdeka Barat No.9
Jakarta Pusat,
10110 Jakarta,
Indonesia

Dear Minister Budi Arie Setiadi

**Subject: Asia Internet Coalition (AIC) Comments on the Draft Electronic Information and
Transactions Law (ITE Law)**

We extend our warm greetings to you and the esteemed members of the Ministry of Communication and Information Technology (KOMINFO). The Asia Internet Coalition (AIC) appreciates the ongoing efforts to address key concerns related to the Electronic Information and Transactions Law (ITE Law) in Indonesia.

The AIC is a leading industry association of Internet and technology companies that promotes the understanding and resolution of Internet policy issues in the Asia Pacific region. Our mission is to represent the Internet industry and participate in and promote stakeholder dialogue between the public and private sectors, sharing best practices and ideas on Internet technology and the digital economy.

On December 5, 2023, we took note of the parliamentary approval of the draft second amendment to the ITE Law. The AIC recognizes the steps taken to refine the legal definition of defamation, reduce maximum sentences from four to two years, impose a higher burden of proof for charges and that these amendments aim to strike a balance between freedom of expression and considerations of moral, religious, and public order.

While acknowledging these positive developments, we wish to express our ongoing interest and commitment to contributing to the legislative process surrounding the ITE Law. In light of concerns raised by rights organizations regarding the lack of harmonization with the new Criminal Code, we believe that continued dialogue is crucial to achieving a balanced and effective legal framework.

With the aim of fostering an environment conducive to innovation, expression, and the free flow of information, the AIC kindly requests an opportunity to submit further comments on the latest version of the ITE Law as highlighted in Appendix I of this letter. We believe that ongoing collaboration and an open exchange of perspectives will contribute to the refinement of the ITE Law, ensuring it aligns with international best practices and addresses concerns related to freedom of expression.

We understand the complexity of the legislative process and appreciate your dedication to ensuring a legal framework that balances the rights of individuals with broader societal considerations. As such, we greatly appreciate the opportunity to submit additional comments at this stage and would welcome the opportunity for a meeting to discuss our insights further.

Thank you for considering our request. We remain committed to constructive engagement and look forward to the continued collaboration between the AIC and KOMINFO. Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Furthermore, we would also be happy to offer our inputs and insights on industry best practices, directly through discussions and help shape the dialogue for the advancement of Indonesia's digital economy.

Thank you
Sincerely,



Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

**Detailed Comments on the Electronic Information and Transactions Law (ITE Law)
Amendment**

Chapter	Comments and Recommendations
Chapter 16A (Child Age verification) (1) Electronic System Operators are obliged to provide protection for children who use or access the Electronic System. (2) Protection as intended in paragraph (1) includes protection of children's rights as intended in statutory regulations regarding the use of products, services and features developed and operated by Electronic System Operators. (3) In providing products, services and features for children, Electronic System Operators are required to implement technology and operational technical measures to provide protection as intended in paragraph (1) from the development stage to the Electronic System implementation stage. (4) In providing protection as intended in paragraph (1), Electronic System Operators are required to provide: - information regarding the minimum age limit for children who can use the product or service; - child user verification mechanism; And - mechanism for reporting abuse of products, services and features that violate or have the potential to violate children's rights. (5) Further provisions regarding protection as intended in paragraph (1) to paragraph (4) are regulated in Government Regulations.	- We suggest “Children” be changed to “Minors” as a more appropriate term so that we can differentiate children from minors. Since some services are not intended for children and require that the person must be at least 13 years old to create an account, it is important that the definition, such as “minors” can better reflect such differences. - Foreign organizations or individuals have existing processes to respond to complained contents. KOMINFO should look into existing available processes that are already accessible to the public globally. Since existing policies and services should cover the requirement under Chapter 16A; - The requirement for age verification should apply to the extent of technical possibility and for different social media platforms and business models that may not focus on minors. It is important to not focus on one set of requirements for all companies. - The Decree must be able to address how the KOMINFO can ensure clear harmonized standards for safeguarding and processing personal data, supplemented by regulatory guidance as new issues emerge, recognizing that it is neither feasible nor desirable to legislate for every potential scenario of how personal data is used for child protection. - There is an urgent need to consult and include the relevant stakeholders to ensure that the law will not violate the right to privacy and that safeguards are in place to avoid personal data breaches and unauthorized processing of personal data for children. - The definition of and threshold for the words “child” and “of age” under Indonesian law and regulations currently vary, ranging from 16, 18, to 21 years old and even with additional

Chapter	Comments and Recommendations
	conditions such as “or have yet to marry”. Electronic Service Providers (ESPs) will be in an uncertain position when implementing their child protection policies, since any failure to adequately consider this factor could lead to the possible imposition of sanctions or seeking of damages.
Chapter 18A (International Contract) and its Elucidation part (1) International Electronic Contracts that use standard clauses made by Electronic System Operators are regulated by Indonesian law in terms of: - the user of the Electronic System Operator's services as a party to the Electronic Transaction originates from Indonesia and gives his/her consent from or within the jurisdiction of Indonesia; - the place of execution of the contract is in the territory of Indonesia; and/or - The Electronic System Operator has a place of business or carries out business activities in the territory of Indonesia. (2) Electronic Contracts as intended in paragraph (1) use simple, clear and easy to understand language, and uphold the principles of good faith and transparency	The Bill states that the requirements will be applicable in line with the following conditions: (1) Products, services or Systems organized by ESPs that are utilized or accessed by users who are located in Indonesia; (2) ESPs have representative offices in Indonesia or in an Indonesian business entity; and/or (3) ESPs offer services or products and have drawn up terms and conditions for the use of services in Bahasa Indonesia or by targeting Indonesian citizens as their market, to guarantee better access for Indonesians to an effective and efficient legal system in any dispute. - Does that mean the ESPs terms and conditions must refer to Indonesian law as the governing law? - How can a reference to Indonesian law guarantee an effective and efficient legal system to users?
Chapter 27 (Decency) (1) Every person intentionally and without right broadcasts, displays, distributes, transmits and/or makes accessible Electronic Information and/or Electronic Documents that have content that violates decency for public knowledge. (2) Every person intentionally and without authorization distributes, transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain gambling content.	• The ITE should be able to provide a clear and transparent list of possible violations to avoid any ambiguity. • The term “decency” is broad and subject to interpretation. • Foreign organizations or individuals have existing processes to respond to complained contents. KOMINFO should look into these existing available processes that are already accessible to the public globally. • The Decree should allow foreign organizations or individuals providing information across the border to act on the complained content on a reasonably expeditious basis. This move takes into consideration human review for content that may be subjective and contextual.

Chapter	Comments and Recommendations
Chapter 28 (False information, Misinformation, Discrimination, Dehumanization and Public Order) - Any Person intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notices or misleading information which results in material losses for consumers in Electronic Transactions. - Any Person intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents that are inciting, inviting, or influencing other people so as to create feelings of hatred or enmity towards certain individuals and/or community groups based on race, nationality, ethnicity, skin color, religion, creed, gender, mental disability, or physical disability. - Every person deliberately distributes electronic information and/or electronic documents which he knows contain false notifications that cause unrest in society.	- Content moderation is more than just ‘leave up or take down’. Regulation should allow for a range of interventions, while setting clear definitions for categories of content. There are several overlapping laws and regulations that are already in place in Indonesia that deal with the requirement under Chapter 28. - Providing users with context, whether concerning an account, piece of content, or form of engagement, is more informative to the broader public conversation than removing content while providing controls to people and communities to control their own experience is empowering and impactful. - It is important that due process should be observed and clearly identified on how KOMINFO will use their authority and should not be given broad discretion to determine what content can be blocked/removed without judicial oversight. - Where the content at issue is lawful, but KOMINFO believes there’s a need to intervene, the regulatory framework under ITE should clearly distinguish between these types of content. - Foreign organizations or individuals have existing processes to enforce their Rules and Policies. KOMINFO should look into these existing available processes that are already accessible to the public globally. Additionally, they also already have dedicated law enforcement channels which are available 24/7 in which KOMINFO should use to make a legal request.
Chapter 40A - The government is responsible for encouraging the creation of a digital ecosystem that is fair, accountable, safe, and innovative. - In order to carry out the responsibilities as intended in paragraph (1), the Government has the authority to order Electronic System Operators to make adjustments to the Electronic System and/or take certain actions.	- The ITE should set clear guidelines for content takedown to ensure transparency that enables accountability for foreign organizations and individuals, as well as the Ministry. In addition, it should address how different law enforcement will use different and existing laws for content moderation. - Due process requires that decisions made by the KOMINFO should be appealable before judicial proceedings in administrative courts.

Chapter	Comments and Recommendations
- Electronic System Operators are obliged to carry out orders as intended in paragraph (2). - In the event that the Electronic System Operator violates the obligations as intended in paragraph (3), the Electronic System Operator will be subject to administrative sanctions. - Administrative sanctions as intended in paragraph (4) can be in the form of: - written warning; - administrative fines; - temporary suspension; and/or - Termination of Access. - Further provisions regarding the responsibilities as intended in paragraph (1), the authority of the Government as intended in paragraph (2), the obligations of Electronic System Operators as intended in paragraph (3), and the imposition of administrative sanctions as intended in paragraph (4) and paragraph (5) regulated in Government Regulations.	This should be provided and expressly guaranteed within ITE law. - Due process must be provided and expressly guaranteed within the Decree as regards any order for locking or deletion of any content to given social media companies to comply under Chapter 40. - To provide clear explanation and transparent procedures for administrative sanctions, such as how KOMINFO legal powers and discretions will be used. - Foreign organizations or individuals have existing processes to enforce their Rules and Policies. KOMINFO should look into these existing available processes that are already accessible to the public globally. Additionally, they also already have dedicated law enforcement channels which are available 24/7 in which KOMINFO should use existing process to make a legal request.
Elucidation of Chapter 40 A paragraph (2) <i>“The authority of the government to issue orders demanding Systems adjustments to ESPs, which must be complied with by ESPs. Adjustments that may be ordered by the government include the limitation or addition of software or hardware features within Systems.”</i>	<i>“The authority of the government to issue orders demanding Systems adjustments to ESPs, which must be complied with by ESPs. Adjustments that may be ordered by the government include the limitation or addition of software or hardware features within Systems.”</i> This adds to uncertainty of doing business in the country and places ESPs in a position where the adjustment, removal of, or addition of software by the Government may compromise the level of protection privacy What would be the legal basis of such an order to adjust, limit or add any software? The country may be perceived as state ruled by power instead by law Chapter 40 (2) (c) and (d) mandate proactive monitoring of illegal content, limiting the intermediary liability protection.