5 September 2022

Mr. Yaw-Shyang Chen
Chairman
National Communications Commission
No.50, Sec. 1, RenAi Rd.,
Taipei City 10052,
Taiwan

Subject: Asia Internet Coalition (AIC) Comments and Recommendations on the Digital Intermediary Service Act ("DISA"), Taiwan

The Asia Internet Coalition (AIC) and its Members wish to express our sincere gratitude to the National Communications Commission (NCC) for the opportunity to submit comments on Taiwan's bill of the Digital Intermediary Service Act (DISA).

The AIC is an industry association of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region.

First and foremost, we commend the NCC for their efforts on drafting the DISA which will look to remove illegal contents, improve transparency, and service terms to protect users' rights. At the same time, the objectives for any reforms should be to avoid unnecessary compliance burdens, promote ease of doing business, and provide more certain and well-understood obligations for platforms. While we support the NCC's intention, we would also like to express some concerns on this draft Bill as its implementation may effectively end the light touch regulatory environment for digital providers in Taiwan by increasing costs and regulatory burdens without clear benefits to consumers. As such, please find appended to this letter, detailed comments and recommendations, which we would like the NCC to consider before proceeding further with the bill.

A global observation we wish to offer is that to the extent that the DISA proposals are transplanted from regulatory developments overseas, it is important to understand those proposals reflect very different political, economic, and legal contexts. For example, the European legislation referenced was drafted to support the European common market and the concepts used reflect European legal concepts. It is also worth noting that some of the more recent regulatory developments have long transition and implementation periods. It will therefore be some time before anyone will be able to determine whether these new and experimental regulations will work and deliver the benefits claimed. For this reason, many other jurisdictions are approaching these developments with

caution, with some preferring to wait and see how these developments work out. Some regulatory agencies like the UK CMA have raised concerns about the degree to which the more heavy-handed regulatory developments could impede investment and innovation. We urge NCC to pause to observe how these regulatory experiments unfold. This seems more prudent than rushing to adopt a foreign regulator model and could avoid potentially adverse consequences for Taiwanese consumers or the economy overall.

We are also grateful to the NCC for upholding a transparent, multi-stakeholder approach in developing this Act. We further welcome the opportunity to offer our inputs and insights, directly through meetings and participating in the official consultations.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Details Comments and Recommendations

1. **Article 2:** AIC wishes to seek further clarity on definition and product in scope under the DISA, especially the definition of mere conduit services, caching services, hosting services and online platform services.

2. **Article 14: DI service providers without a commercial presence in Taiwan shall designate an agent in Taiwan and report the same to the NCC**

   The obligation to designate an agent in Taiwan who will be responsible for "legal compliance matters" and that any violations of the agent would be considered a violation by the digital service provider is a concern. Internet platforms, by its very nature of business, are transnational in nature. It has been successfully demonstrated that often the expected outcome i.e. transparency report, user rights etc. can be achieved without designation of a local agent. It will be useful if further clarity about the need and scope of the role of the designate agent can be provided by the government.

   Furthermore, any requirement for companies to designate an agent in Taiwan may impose unnecessary, expensive, and inappropriate requirements on companies providing goods or services digitally—hurting SMEs most of all. Key concerns include:

   - **Reduce competitiveness of a nation:** While many governments see these policies as simple solutions to the challenges of a complex global economy, the truth is that the drawbacks for a country and its companies far outweigh the benefits. Instead, localization efforts reduce that country's competitiveness across all local economic sectors and undermine the health of the global economy by raising the cost of doing business internationally.
   - **Restrict Growth of SMEs and Stifle Innovation:** Local presence requirements artificially restrict SMEs' market and growth prospects by limiting their ability to engage potential partners and resources. SMEs rarely have the resources to invest in local offices or appointment in every market to which they seek to expand digitally.
   - **Against international trade norms:** By instituting local presence requirements, countries are deviating from established international trade norms and practices, that promote free trade, by erecting unnecessary barriers to cross-border services trade.
   - **Onerous costs and administrative challenges:** Agent designation increases compliance costs for companies.

To minimize unnecessary regulatory compliance costs but achieve the objective the NCC could consider a range of alternative measures, for example to identified a dedicated point of contract which may not need to be a physical agent in Taiwan.

3. **Article 16: DI service providers shall regularly publicize their transparency reports in a clear and easily comprehensible manner each year, disclosing information on government requests for user data, actions taken towards illegal content, self-regulatory code, etc. (however, DI service providers below a certain threshold can be exempted from the aforesaid requirement)**

    a. *In addition to the information referred to in Article 16, online platform service providers shall include the information on complaints and Misuses they handled, explanation of any use of automated means for content moderation, etc. in their transparency reports (Article 29 of the DISA).*

- Many of our members publish transparency reports on their enforcement efforts. Some examples include Apple; Facebook, Google, LINE and YouTube; Yahoo; Twitter. On this note, the AIC wishes to seek clarity on the language of the transparency report.
- Secondly, Section 5 requires "Cooperation mechanism with third-party fact-checking organizations". It is not clear whether such cooperation is required on an ongoing basis, as an audit mechanism or for any other purpose. If mandatory, this is a very specific and prescriptive requirement. It would be helpful to understand what outcome is proposed to be achieved from such cooperation and perhaps the process by which such outcome is achieved should be left with the platforms themselves.
- Based on our members' experience with annual transparency reports, there are a few points we would highlight going forward when considering any specific rules on transparency reporting:
    - There should not be an obligation on service providers to report on the exact types of automated tools used or the details of their functionalities.
    - Transparency around outcomes and actions can still be useful, but disclosing too much about how a service provider takes a particular enforcement action can inadvertently provide a guide to bad actors to game their systems.
    - Any specific rules on the frequency of transparency reports will require operational changes from service providers, which may be too

burdensome for some service providers. Furthermore, should reports be requested too frequently they could be ineffective as it will be impossible to analyze the data and to draw conclusions within unrealistic timelines.

- Regarding the content of any transparency reports, we would advise against the consideration of any horizontal template for transparency reporting across businesses and online service providers - as this will not achieve the desired effect and will not sufficiently take account of the nuances of different service offerings. Proportionality should instead be the key indicator for transparency reports going forward.
- There should not be obligations on the service provider to provide detailed reporting on the status of different user flags and notices. Many user flags are inaccurate or abusive, and a service provider needs to be flexible in its response to take account of these challenges. Rules on reporting the exact turn around time of flags, or information about each step in the process for each flag would hamper this flexibility.

4. **Article 17: DI service providers shall, in accordance with laws, provide the government with the information about one or more specific recipients of their services that they stored for the purposes of providing such services**

   Regarding the points on systemically responding to law enforcement authorities and cooperation with national authorities, we understand the legitimate interests of law enforcement, but we would be concerned about proposals that would circumvent existing legal protections or require online service providers to disclose user data to the government without any prior oversight by an independent authority and without proper safeguards

5. **Articles 18 through 21: When any competent authority (i) with respect to the information transmitted or stored by a DI service provider as requested by a recipient of the service, obtains from the court an access restriction order or emergency access restriction order; or (ii) with respect to the information stored and disseminated to the public by a DI service provider as requested by a recipient of the service, imposes an interim warning annotation measure, such DI service provider shall comply with said order or measure and publish such decisions with respect to restrictions on information flows on the publicly accessible database managed by the NCC for public searches.**

   - [ISPs / hosting service providers/ Internet intermediaries / social media companies] always assess the legitimacy and completeness of a government

request. In order for [ISPs / hosting service providers/ Internet intermediaries / social media companies] to evaluate a request, it must be in writing, as specific as possible about the content to be removed, and clear in its explanation of how the content is illegal with legal basis.. [ISPs / hosting service providers/ Internet intermediaries / social media companies] will not honor requests that have not been made through the appropriate channels and supporting evidence for the request

- There are many reasons why [ISPs / hosting service providers/ Internet intermediaries / social media companies] cannot impose a warning to remove the content or restrict access of the content.
    - Some requests might not be specific enough for [ISPs / hosting service providers/ Internet intermediaries / social media companies] to know what the government wants them to warn on. Also, hosting service providers who merely provide underlining infrastructural storage services or computing services do not have control over, or visibility into, or knowledge of the content stored by their customers so that they cannot impose a warning.
    - In these cases, [ISPs / hosting service providers/ Internet intermediaries / social media companies] ask for more information. Other times, [ISPs / hosting service providers/ Internet intermediaries / social media companies] don't take action because the content has already been removed by the content owner.
    - Sometimes [ISPs / hosting service providers/ Internet intermediaries / social media companies] receive overly broad requests from both end-users and government agencies.
    - Also, for hosting service providers who merely provide underlining infrastructural storage services or computing services, given that they do not have control over, or visibility into, or knowledge of the content stored by their customers, they cannot take actions against a specific content. They should be allowed to forward these requests or notification to their customers or other third parties who have control over the uploaded content to take actions against a specific content.
- The system in place should have clear formalities for submitting notices:
    - Clearly identify the content at issue by URL and where applicable, include video timestamp, or some other unique identifier (not a second-level domain);
    - Clearly state the basis of the legal claim, including the provisions of the applicable local laws and the country in which the law applies;

- Clearly identify the sender of notice, especially where the nature of the rights asserted requires identification of the rightsholder, the request should come from an official Government source (email or letter); and
- Attest to the good faith and validity of the claim using the legal form appropriate to the jurisdiction (such as an oath under penalty of perjury) with penalties for notices issued in bad faith.

6. **Article 30: When displaying advertising on their online interfaces, online platform service providers shall indicate in a clear, conspicuous, real-time identifiable manner that the information displayed is an advertisement, disclose the advertiser on whose behalf the advertisement is displayed, and provide information on the main parameters used to determine the recipients to whom the advertisement is displayed so that recipients of their services can understand why an advertisement would be displayed to them.**

   - It is unclear what the obligation in (3) relates to ("Information to determine the main parameters of advertising display objects"). It would be helpful to clarify this.
   - Most ad recommender mechanism are based on hundreds of cues based on user behavior and sharing these with the user each time an ad is displayed is likely to not only adversely impact the user experience, induce information fatigue but also allow advertisers to 'game' the system which will be to the detriment of the user.
   - We would like to recommend that this article may be harmonized with DSA as this may be intended as an identical "main parameters" obligation.

7. **Article 32: The DISA imposes general obligations with respect to all DI service providers as well as special obligations specifically for hosting service providers and online platform service providers. Furthermore, the DISA also authorizes the NCC to designate online platform service providers with 2.3 million active recipients of their services within the territory of Taiwan as "Designated Online Platform Service Providers" and imposes additional obligations on them**

   - We have concerns that designation proposal for online platform service providers, while superficially appealing, conceals a number of real world difficulties and raise fairness issues.
   - First, it is a core principle of regulatory design that new regulation should be introduced where there is a need. In this context, there is no assessment of

whether online platform service providers with 2.3 million users are "gatekeepers". The reason behind designation is a concern that the business has enduring power which is unlikely to be removed by competition and/or users have no choice. If that is not the case, there is a real question as to why designation is needed. The guiding principle is that designation should only cover businesses that truly are "gatekeepers" and this suggests the NCC should consider carefully the nature of service involved, the extent to which users have alternative choices. For example, are restaurant reviews, music streaming, or online retail services that satisfy the market power requirement noted above. Criteria such as the number of users of a service are not a principle way of determining whether any given business is actually a "gatekeeper".

- Second, if there is a "gatekeeper," designation should provide businesses with certainty. An approach that relies purely on quantitative thresholds such as turnover figures or the use of a service will tend to arbitrariness and cover some businesses while excluding others, especially where different sectors and business models are covered. For example, a concept like "active recipients" raises what constitutes a "visit" to a platform and as a visit will depend on the service provided. Take a music streaming service. Is each time the streaming service is used to play a song counted as one visit? Or, will opening a new tab in a browser during the same session constitute one visit or two? Before adopting what may appear to be a simple metric it is crucial to understand the differences and complexities involved.
- Third, if introducing designation criteria creates uncertainty for both Taiwanese and international businesses and compliance becomes overly complicated (eg, what is a user) and costly, the most likely outcome is reduced innovation and investment. If a business is not a gatekeeper (i.e. there is a lack of contestability or choice) but is designated that business will be constrained in their ability to innovate and use their assets to deliver the best possible consumer experience.
- Finally, any designation should be fair to avoid distortions across like service providers. This means that: (i) Designation should involve a process where a business can show why they do not meet the core requirement for designation and/or why the criteria do not work (as noted above, what is a user is more complicated than it appears. (ii) Designation should also not unfairly target some businesses but not others. If designation is used to increase costs and make doing business more difficult for some businesses, the longer term outcome is likely to be reduced choice and services available to Taiwanese consumers.

8. **Article 35: Designated Online Platform Service Providers shall engage a third-party independent institution or organization to conduct an audit on their compliance with the general and special obligations described above and implementation of their self-regulation mechanism, and submit an audit report to the NCC.**

   - There is an important role for international standards for compliance frameworks related to addressing illegal content, and we are advocating that the NCC explore including mechanisms in the DISA that support the development within international standards. (We would note that online service providers successfully leverage an array of compliance frameworks for security, privacy, finance, trade etc.)
   - We also wish to seek clarity on whether the audit requirement will need to be aligned to Taiwan law. Ultimately, the complexity of complying with fragmented requirements from third-party independent institutions or organizations can be unduly burdensome, and makes compliance challenging for service providers.

9. **Article 36: Designated Online Platform Service Providers that use recommender systems shall set out in their terms and conditions, in a clear and easily comprehensible manner, the main parameters used in such recommender systems, the options for recipients of their services to modify or adjust those main parameters that they have made available, and the effects from such modification or adjustment. Moreover, the aforesaid options shall include at least one option which is not based on profiling.**

   Regulatory proposals involve a trade-off between providing a framework that benefits innovation, investment and consumers and imposing a more detailed complex regulatory regime that imposes costs on business (which can ultimately leading to reduced investment and innovation). We have described some of the trade-offs below.

   i. *Pros of platform services*:(a) The personalisation of platform services tailored to the user's choice e.g. music, entertainment streaming, or retail services is something users value very highly. Regulation could remove the incentives to innovate to produce these kinds of personalisation algorithms. (b) It is also well accepted that consumers benefit from tools that help them to reduce their search costs such as algorithms. The lower the consumer's search costs the more time consumers have to allocate to other tasks including pursuing different choices. (c) It is also accepted that platform users should not be in a position to "game" the algorithms. Public disclosures may give bad or adversarial actors the information they need to game the system, avoiding platforms' mechanisms for fighting spam

and launching coordinated inauthentic behavior. For example, forcing disclosure of the algorithm that identifies fake products on a retail site would lead to bad actors being able to game the algorithm, to sell more fake products, which reduces the benefits to consumers. (d) It is also costly to develop or improve algorithms. Forced disclosure of the main parameters used in an algorithm could reduce incentives to develop or improve algorithms. Disclosing the main components or parameters provides an insight that competitors would not otherwise have, which could turn businesses away from future investments.

ii. *Cons of platform services*. If algorithms or processes make decisions for consumers, the argument is that this makes it harder for users to their ranking or understand decisions being made.

Before requiring digital businesses to disclose the main parameters used in its algorithmic recommendations, or giving options for users to modify those parameters the NCC must consider factors like: (i) what risks platforms pose, (ii) what specific disclosures and burdens are appropriate as a result, and (iii) what goals justify disclosure mandates. If, after undertaking this pros/cons analysis a disclosure mandate is proposed there needs to be an exemption process. If a business can demonstrate why the mandate does not deliver benefits to consumers claimed or involves certain risks, allowing a business to opt out of the recommender system or only having the mandate applied only to very select services should be included in any proposed reforms.

However, by far, the preferable outcome would be to wait and see how such mandates work in the EU before importing such a mandate to Taiwan.

10. Implementation Timeline

Internet platforms are focused on user safety and are continuously introducing new measures and learning from responses to existing measures including providing language support across different countries. For any changes that may be required there is a need for adequate time to implement changed compliance obligations with respect to carrying multiple language support. It is therefore requested that sufficient time may be given (18-24 months) to platforms to put in place a robust content moderation mechanism that supports Chinese language.