

Asia Internet Coalition (AIC) Industry Comments on Taiwan Anti Scam Code and Implementing Guidelines

29 October 2024

Honourable Minister Yennun Huang,
Ministry of Digital Affairs (MODA),
No. 143, Yanping S. Rd.,
Zhongzheng Dist., Taipei City 100057, Taiwan (R.O.C.)

Dear Minister Yennun Huang,

The Asia Internet Coalition (AIC) is pleased to submit our comments and recommendations regarding the Taiwan Anti-Scam Code and its Implementing Guidelines. We greatly appreciate the Ministry of Digital Affairs' inclusive approach in consulting with industry stakeholders on these important initiatives aimed at enhancing Taiwan's digital economy.

As an association of leading Internet and technology companies in the Asia-Pacific, the AIC is dedicated to promoting balanced Internet policy and fostering cooperation between public and private sectors to develop effective digital governance. Our submission in **Appendix I** provides detailed insights and recommendations on key elements of the proposed guidelines, including [take-down requests](#), [disclosure requirements](#), and [verification standards for online advertising platforms](#).

We hope our contributions will support MODA's efforts in implementing robust, effective anti-scam measures, and we remain available to discuss our recommendations in further detail. Should there be any questions, please feel free to reach out to Mr. Sarthak Luthra at **Secretariat@aicasia.org**.

Thank you for the opportunity to participate in this important dialogue. We look forward to continued collaboration with MODA to advance Taiwan's digital economy.

Sincerely,

Secretariat
Asia Internet Coalition (AIC)
<https://aicasia.org>

APPENDIX I

1. 24-Hour Turnaround Time

Imposing a rigid 24-hour turnaround time (TAT) for responding to takedown requests, as proposed in Taiwan's Anti - Fraud Act (AFA) implementing regulations, poses significant challenges for intermediaries and risks undermining both efficiency and fairness. Internet intermediaries regularly receive a high volume of requests, many of which are overly broad or lack specificity, making immediate action impractical. Also, given the complex nature of scams, further investigation may be required before action can be taken. An arbitrary 24-hour deadline could lead to overblocking of legitimate content, especially if there's insufficient time to thoroughly assess the legality of the material. Further to this, offshore platforms rely on local representatives to receive Takedown Requests ("TDRs") under the Taiwan AFA, and such local reps may not provide 24/7 support and weekend coverage. The added layer of local rep as a service agent makes the 24h TAT extremely challenging to meet.

It is also essential to note that having companies focus on TAT does not necessarily result in the reduction of scam harm, and a rigid TAT regime without flexibility may result in companies shifting resources away from proactive and longer-term work to detect scams and the networks behind them and towards a more reactive, 'whack-a-mole' approach based on takedown requests. A more nuanced approach that focuses on transparency, fairness, and proportionality will not only reduce harmful content but also ensure that legitimate speech is not unjustly censored.

Further, requiring intermediaries to act within strict, short deadlines without proper assessment could violate international norms on freedom of expression. A more nuanced approach—focusing on transparency, fairness, and proportionality—will not only reduce harmful content but also ensure that legitimate speech is not unjustly censored.

Recommendations:

- To prevent the pitfalls as described above, the law should avoid imposing rigid timeframes and instead encourage responses "within a reasonable timeframe" or "without undue delay." This would allow intermediaries to carry out thorough assessments while maintaining a balance between speed, accuracy and efficacy.
- To ensure the added layer of a local rep does not prolong the process unnecessarily, we recommend incorporating early signaling mechanisms for intermediaries to be *unofficially* notified in advance of a takedown notice being issued to the designated online webform or local rep / service agent. This would allow platforms to have more time to work on requests and prepare for potential actions. Such early signaling, however, should be clearly distinguished

from an official Takedown Request (TDR) order, ensuring that platforms understand the difference and do not take premature action based on preliminary notifications.

- If a 24-hour timeline is to be implemented, it should only apply when a legally valid and complete order is received by the platform, allowing them to act swiftly upon receipt. In cases where platforms require additional information (e.g. insufficient information to locate the reported ads) or need to conduct further investigation, the 24-hour clock should either not start or be paused until all necessary details are provided, enabling informed decision-making and minimizing the risk of unwarranted takedowns.

2. Advertiser Verification Standards and On-Ad Disclosures

Firstly, it is important to note that combating online scams requires a comprehensive approach, including having a robust set of policies, enforcement practices, consumer safety tools, awareness and education campaigns, and cross-industry and multi-stakeholder partnerships. Verification is only one of many measures that contribute to safeguarding the advertising ecosystem. As such, advertiser verification frameworks should adopt a balanced approach that strikes a balance between access, privacy, and consumer safety.

The implementing rules and the parent obligations relating to advertiser verification risks disproportionately penalizing many legitimate advertisers by creating barriers for access, as well as potentially exposing individual users that are running ads (such as sole proprietors) to additional risks of privacy and safety-related harms, due to the payer and beneficiary disclosure requirement in which individual's information would be displayed. Advertisers consist of large brands and corporations to sole proprietors and individuals who run ads for a variety of reasons, not only to promote a product or service, but also for personal, charitable or other causes. Requiring individuals to disclose their personal information as a payer or beneficiary exposes them as a potential target for abuse, or even deter them from advertising altogether.

Recommendations:

We recommend that the implementing rules work to address concerns regarding access, proportionality and individual users' privacy by taking an approach that focuses on transparency, fairness, and proportionality. To achieve this, we recommend the implementing guidelines incorporate several key principles:

- **Effectiveness:** Deploy targeted, risk-based solutions that can effectively address the potential risk of scam harm.
- **Targeted and risk-based:** Apply more restrictive rules in targeted scenarios where there may be signals of a potentially inauthentic or malicious actor or where there may be a higher risk of

scam harm and users being targeted, for example to advertise certain highly regulated goods and services may require additional verification steps.

- **Proportionate:** Apply stricter measures where there is evidence of potential scam harm and where the potential for scam harm increases, rather than employing a blanket or overinclusive approach that would disproportionately disrupt access and economic opportunity for legitimate advertisers.
- **Flexible:** Build verification solutions that are able to quickly adapt to the continuously evolving threat landscape and rapidly changing adversarial tactics of malicious actors.
- **Data protection & privacy:** Adhere to global data minimization standards in which the minimum amount of data should be collected, stored and used to prove the authenticity of advertisers. Be transparent about when and why additional user data is collected, retained and displayed (i.e. where it doesn't put users at risk) to prevent the potential for harm.

3. Annual Transparency Fraud Report

While we support transparency reporting, it is essential that such reporting is meaningful and focuses on outcomes that are tailored to the specific institutional arrangements of the respective jurisdiction. Requiring platforms to disclose granular metrics like monthly active users (MAUs), for example, raises concerns about overexposing sensitive business information, without contributing significantly to fraud prevention. MAUs are competitive metrics, and mandating their disclosure could unfairly compromise platforms' strategic positions while offering little value in addressing fraud.

We also note that the transparency report under Art 30 II (2) limits the scope to cover advertising services only. Furthermore, user-generated content (UGC), as outlined in Art 33, should be out of scope of transparency reporting requirements.

Transparency should aim to provide relevant insights directly tied to fraud mitigation efforts. Overbroad requirements that focus on irrelevant or overly detailed data may result in information overload, confusing stakeholders and diluting the focus on actionable fraud prevention measures. A targeted, outcomes and risk-based approach ensures transparency reports are tailored to the actual challenges within the jurisdiction and provide meaningful information to regulators, policymakers, and the public. Moreover, transparency measures should not inadvertently expose platforms to risks by offering bad actors insights into operational details.

Focusing on outcomes-based reporting—such as the effectiveness of fraud detection and prevention mechanisms—ensures that transparency serves its intended purpose while protecting the integrity of platforms and user privacy. This approach supports the development of regulatory frameworks that are proportional, flexible, and adaptable to the local context, allowing platforms to report on measures that genuinely contribute to online safety.

Further, information on “other items” in which competent authorities of the digital economy-related industries may request, as provided in the implementing guidelines, should be clarified. As currently

drafted, intermediaries may be unable to properly plan and prepare for the annual transparency report if competent authorities may require additional information at their discretion.

Recommendations:

- We recommend that the annual transparency report be limited to intermediaries only providing meaningful information on their fraud prevention plan, where disclosure of such information would not compromise the safety of users and the integrity of companies' systems, nor require companies to disclose trade secrets. As such, the requirement to provide Monthly Active Users, and average processing time should be removed, as it does not provide any meaningful information on intermediaries' fraud prevention efforts.
- Additionally, intermediaries should only be required to report statistics on intermediaries' action rates in response to legal takedown requests which are related to advertising services only, but not UGC contents.
- We also recommend that clear criteria and guardrails are established for "competent authorities" attempting to expand the scope of the transparency report. Requirements to report on "other items" should be limited to intermediaries' fraud prevention plan and handling of legal takedown requests related to the advertising business, and provide for a reasonable time period for intermediaries to provide such information. Additionally, competent authorities should be required to first consult with intermediaries on the addition of "other items" to the transparency report to ensure the information requested is appropriate and feasible.

4. Legal TDR and Potential TDR Portal

Technologies used to facilitate intermediaries' obligations with local law should ensure that it fairly and efficiently helps facilitate compliance. In the case of technologies used for the handling of takedown requests (TDRs), it is important that it does not disrupt and negatively impact the government and platform's abilities to expeditiously handle these requests. As such, we recommend that the development and implementation of TDR technologies be guided by the following principles:

1. **Consultations and Feedback:** The TDR portal should be developed using best practices in system design and software engineering to minimize failures, particularly during critical periods, such as elections or heightened scam activity. Implementing multiple testing phases and soliciting extensive feedback from stakeholders will ensure that the portal is fit for purpose, promoting high adoption rates and compliance while reducing the risk of costly system failures. Further to this, TDR portals should be developed with extensive feedback and consultation with entities who are subject to the use of the portal to ensure that it is built to be fit for purpose with high adoption and compliance rates.

2. **Due Process:** The TDRs and TDR portal must incorporate mechanisms that uphold the principles of due process. This includes ensuring procedural safeguards that protect individuals' rights to fair treatment and natural justice, preventing arbitrary decision-making. All parties involved in the TDR process should have access to clear guidelines outlining their rights and responsibilities, thereby fostering a sense of fairness and transparency.
3. **Freedom of Expression:** It is essential that the TDRs and TDR portal align with international human rights standards, particularly regarding freedom of expression. To uphold these standards, takedown requests issued by the TDR portal should be complete, valid and provide all necessary information for intermediaries to process. TDRs, at minimum, should include the legal reasoning, the specific law or provision allegedly violated, and detailed information about the content in question (such as the URL, screenshot or other information needed to easily identify the content), and should be issued by a competent authority. Where the report is submitted by users - authorities need to conduct a substantive review of the reported content and confirm if such content is locally unlawful before issuing a TDR. Such due diligence ensures that the restriction of content is based on sound legal grounds.
4. **Privacy, Data, and Infrastructure Security:** The TDR portal must adhere to established global privacy and data security principles. This includes implementing robust measures for collecting, storing, and transmitting user data securely. Moreover, the infrastructure supporting the TDR portal should be fortified against cyber threats, including DDoS attacks and malware, to protect sensitive data from breaches that could have serious legal and operational consequences.
5. **System Interface:** To facilitate efficient and effective communication between the government and online platforms, it is essential to develop a standardized system interface, such as an Application Programming Interface (API). This API should be built in consultation with the tech industry to ensure that it meets industry standards and is fit for purpose. A well-designed API will enable seamless information exchange, reduce errors, and streamline processes. We recommend that an open dialogue with platforms to develop such interfaces, leveraging the expertise and experience of both parties to create a robust and reliable system.
6. **Efficiency & Consistency:** The TDR portal should enhance operational efficiency for both regulators and platforms without increasing the compliance burden. A centralized intake platform for all government takedown requests will provide consistency in application of the law and streamline processes. By minimizing administrative overhead, the portal can facilitate faster responses to illegal content while ensuring that the law is applied uniformly across jurisdictions.
7. **Tracking & Compliance:** To ensure accountability, the TDR portal should have robust tracking and logging capabilities that accurately record key activities related to takedown requests. This includes maintaining comprehensive records of case information, submission dates, and correspondence. Such tracking is vital for assessing compliance and identifying areas for improvement in the system.
8. **Availability & Scalability:** The TDR portal must be designed for high availability, with technical support in place to minimize downtime. It should be able to scale effectively to manage fluctuating volumes of requests, particularly during critical events. Furthermore, robust

contingency protocols should be established to address any unplanned outages swiftly, ensuring the portal remains operational and accessible when users need it most.
