

11 July 2024

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

Dear Minister Yennun Huang,

Subject: Asia Internet Coalition (AIC)'s Industry Issues and Recommendations Regarding the Anti-Fraud Act

The Asia Internet Coalition (AIC) 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.

We write to you to express our concerns regarding Taiwan's upcoming *Fraud Crime Hazard Prevention Act*. While we understand and appreciate the importance of combating fraud, we believe that certain provisions within the Act could have significant unintended consequences on the digital ecosystem, international cooperation, and individual privacy. We respectfully urge the Ministry of Digital Affairs (MODA) to consider the following points:

1. **Alignment with Global Best Practices:** It is crucial for the enforcement rules of the Anti-Fraud Act to align with global best practices, particularly regarding advertising obligations. We urge MODA to draw on international standards and frameworks to ensure that Taiwan's regulations do not diverge significantly from those of other leading digital economies. This alignment will help maintain consistency and fairness in the digital advertising landscape, which is essential for fostering innovation and protecting consumer interests.
2. **Legal Conflicts with Other Countries' Laws:** We have identified several legal conflicts between the Anti-Fraud Act and the laws of other countries, which could pose challenges for international cooperation and compliance. As an example, § 37 of the Act, which enables extensive user data requests by Taiwanese law enforcement agencies (LEAs) without judicial oversight, is incompatible with Japan's Constitutional Clause that protects communication secrecy, along with Telecom Business Law, the Personal Data Protection Act (PDPA) and relevant regulations. Moreover, this provision may also conflict with the

privacy laws of other countries, leading to potential legal uncertainties and operational challenges for businesses operating in multiple jurisdictions. The lack of judicial oversight for user data requests by LEAs raises significant privacy and human rights concerns. It is imperative that user privacy is protected through appropriate checks and balances, ensuring that data access by LEAs is subject to judicial review to prevent abuse and uphold human rights standards.

3. **International Consultation and Harmonization:** We strongly urge the Taiwanese government to engage in consultations with other governments to harmonize the enforcement of the Anti-Fraud Act with internationally recognized standards. International cooperation and dialogue are essential to ensure that the Act is implemented in a manner that respects the legal frameworks and privacy protections of other countries, thereby facilitating smoother cross-border digital interactions and fostering trust in Taiwan's regulatory environment.

For ease of reference, we have detailed our concerns and recommendations in Appendix I. 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 Taiwan's digital economy while respecting international norms and protecting individual privacy.

Thank you

Sincerely,



Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

APPENDIX I

1. The bill imposes various obligations on “internet advertising platforms” (hereinafter IAPs), which are defined broadly and with unintended consequences. This definition should be reviewed and narrowed to focus on where fraudulent advertisers enter the digital supply chain and not extend to parties which have no contractual relationship with the advertiser and act as an intermediary. The definition should clarify that private email communication is out of scope of the bill. The current - flawed - definition means some of the obligations extend far beyond advertising services. By such flawed design, the Taiwanese government extends its regulatory reach to the non-ads business of internet service providers when such providers also happen to operate ads businesses. This overreach makes the scope of compliance incomprehensible and confusing, while also lacking justification for these obligations. The nature, risk, and harm of abuse, and the value of freedom of speech on ads content or activities are entirely different from other non-ads content (which includes UGCs) and user activities. These obligations include:
 - a. § 32 I (2) asks IAPs to suspend user accounts involving fraudulent activities. These accounts may not necessarily be “advertiser accounts” but could also be other non-ad service accounts, as the provision and explanatory memorandum suggest.
 - b. § 33 asks IAPs to take down “content,” which is broadly-defined and includes non-ads content such as UGCs, as the explanatory memorandum explicitly states.
 - c. § 38 asks IAPs, along with other service providers, to retain user and transaction data (which may not necessarily be advertising-related data) and to submit data when requested by TW Police, Prosecutors, or Courts within 3 days after being notified. Such requests are not necessarily accompanied by court-issued search warrants.
2. The bill asks IAPs to verify the identity of advertisers and ads funders for ALL kinds of ads (§ 32 II (1)). While the detailed protocol and standard for verification would be determined by TW MODA later, the current legal provision and explanatory memorandum already elaborate digital signatures, FIDO, or on-site inspection as potential protocols, which is a very high and costly standard for operations and will take considerable time to implement. The proportionality of this proposal does not seem to have been considered nor does the bill contemplate grace periods for IAPs to develop and implement such protocols. Such haste surely leads to market turmoil as all players in the

advertising sectors are not able to immediately comply with, and do not know how to comply with, such requirements.

3. The bill also asks IAPs to suspend user accounts involving fraudulent activities, which include accounts of both ads-services and non-ads services, solely upon police notification (§ 32 II (2)). The bill should first recognise that this obligation can only apply to the entity with a contractual relationship with the advertiser. As drafted, this notice-and-suspension protocol, while understandable for timeliness, would not be reviewed by TW courts and does not have a clear user appeal process toward the police.
4. The bill further requires IAPs to remove content relevant to fraud crimes, including UGCs, when notified by the competent authority (i.e., TW MODA) or the police. Although this requirement is not directly backed by penalties toward platforms, it enables the TW government to remove and censor digital contents without review by the courts, by putting pressure on IAPs.
5. The bill asks IAPs and other providers to retain user and transaction data, and to submit data when requested by TW Police, Prosecutors, or Courts within 3 days after being notified, while such requests are not necessarily accompanied by court-issued search warrants. These providers further need to retain requested data for at least 6 months (§ 38). The provisions are problematic for the following four reasons. First of all, the scope of the data is vast and undetermined. Second, the requests are not necessarily reviewed by the courts and are not accompanied by court warrants. This lack of procedural protection is problematic as such data requests infringe on user privacy and should be balanced and checked by proper court review. This lack of protection creates a compliance dilemma across jurisdictions. (For example, JP laws prohibit telecom/internet businesses from submitting data without court warrants when such data is closely relevant to individual communications provided by the business since such data would be deemed as communication secrecy—protected by JP Constitution and Telecom business law.) Third, submission of data within 3 days after being notified is operationally infeasible for most, if not all, service providers, whether they are large or small, foreign or domestic. Finally, further retention for more than 6 months after submission is incomprehensible, as the Courts, Prosecutors, and the Police already receive data after the submission. It is the duty of the state, not of the provider, to carefully preserve and ensure the integrity of obtained evidence, since it is the sovereign that monopolizes the high power of crime investigation, prosecutions, and judiciary.

6. The bill, by asking foreign designated IAPs to appoint a legal representative, creates a direct legal jurisdiction, making the above requirements mandatory for foreign IAPs and creating unresolvable legal conflicts across jurisdictions.
7. The bill also grants the TW government unitary power to perform “traffic management” (i.e., downgrade of traffic speed by CDN), along with termination of DNS resolution and “access restriction” (i.e., total service blockage by DNS RPZ or other methods) on designated IAPs, when (a) IAPs fail to appoint local legal representatives, (b) when the representatives fail to notify or to assist designated foreign IAPs (which could potentially cover all of the compliance failures), (c) IAPs fail to take down illegal ads, or (d) IAPs fail to suspend accounts relevant to fraudulent activities. Such regulatory design, while citing the anti-CSAM/NCII laws in Taiwan, does not provide any meaningful justifications and only serves as a compulsory measure for compliance. This regulatory design not only directly violates the principle of a free and open internet committed by the Taiwan government, but also substantiates a dangerous rule-making tendency that further derails and dismantles such principles, rendering them meaningless in Taiwan.
8. The bill imposes joint liability on IAPs for damages arising from action in response to an advertisement. This should be reviewed for proportionality and to ensure primary liability rests with the advertiser. Liability should not extend to parties with no contractual relationship with the advertiser.
9. Finally, while the TW government claims to adhere to good regulatory practices (GRPs) in various trade treaties and agreements, including the U.S.-Taiwan Initiative on 21st-Century Trade, the Taiwanese government fails to follow GRPs during the rule-making process this time. The bill has not been translated into English for accessibility, has not been open for public comments, and has not invited input from various stakeholders before submission to the Legislature. These failures seriously impede meaningful participation by the internet industry and hamper discussion among civil society, yet the TW Government provided no justification. Although the TW Government claimed the severity of fraud, the urgency, and the high social consensus of combating frauds, which no industry players would object to, such a hollow claim does not elaborate on why the urgency should lead to abandoning GRPs. Nor does the claim meaningfully justify the failure to adhere to GRPs to make good laws so that human rights protection is respected, while industry interests are harmonized and balanced with adequate administration of law realized by due process.

黃部長彥男
數位發展部
100057 臺北市中正區延平南路 143 號
臺灣

亞洲網路聯盟就《詐欺犯罪防制條例》表達關切

黃部長鈞鑒

亞洲網路聯盟（The Asia Internet Coalition, AIC，下稱本聯盟）係由領先的網際網路和技術公司組成的產業協會，旨在促進亞太地區對網際網路政策相關議題之認識及溝通。本聯盟致力參與並促進公私部門利害關係人間對話，分享網路技術與數位經濟之最佳實踐與理念。

本聯盟致函表達對臺灣即將通過並生效之《詐欺犯罪危害防制條例》（下稱本條例）之關切。對於詐欺防治之必要，本聯盟敬表贊同，惟本條例特定條文將對數位生態、國際互助及個人隱私權造成重大的非預期後果。本聯盟建請數位發展部，宜請斟酌下列事項：

- 1. 與全球最佳實踐保持一致：**本聯盟呼籲本條例之施行細則，特別是廣告相關義務，應與全球之最佳實踐相符。本聯盟敦促數位發展部借鑑國際標準與框架，確保臺灣相關法規與其他領先之數位經濟體法規不具重大差異。與相關最佳實踐保持一致，有助維持數位廣告領域之一致性與公平性，於促進創新與保護消費者利益至關重要。
- 2. 與他國法律相衝突：**本聯盟留意到本條例與他國法律存在多處法律衝突，進而對國際互助與法遵事務帶來挑戰。例如本條例第 37 條允許臺灣執法機關毋需司法監督即可廣泛向業者調取使用者資料，此規範與日本《日本國憲法》保障通訊秘密之條文、《電信事業法》（電氣通信事業法）與《個人資料保護法》（個人情報の保護に関する法律）及相關法規迥不相侔；該條文亦可能與其他國家隱私相關法律衝突，使業務橫跨多個司法管轄權之業者面臨潛在的法律不確定性及營運挑戰。執法機關調取用戶資料而缺乏司法監督，亦引發嚴重的隱私權與人權問題。使用者隱私至關重要，應受具備適當權力制衡保護，以確保執法機關接觸使用者資料時受司法審查，以避免人權侵害並秉持人權準則。
- 3. 國際諮詢與調和：**本聯盟強烈敦促臺灣政府與他國政府進行諮詢，使本條例之執行實務與國際公認標準相調和。國際互助與對話，對於確保本條例實施時得尊重他

國之法律框架及隱私保護至關重要，從而促進跨境數位互動之順暢，進而增進各國對臺灣管制環境之信任。

為便利參考，本聯盟於本函附錄一詳列具體之關切事項與建議。如後續有疑問或待釐清事項，還請不吝與本聯盟秘書處 Sarthak Luthra 先生聯繫（電郵地址 Secretariat@aicasia.org 或電話 +65 8739 1490）。本聯盟也樂於透過直接討論提供我們的見解和行業最佳實踐，幫助推動臺灣數位經濟的發展，同時尊重國際規範和保護個人隱私。

順頌時祺，



亞洲網路聯盟總經理 Jeff Paine

附錄一

1. 本條例對於「網路廣告平臺業者」（以下簡稱 IAPs）施加了各種義務，但其中一些義務遠遠超出了廣告服務的範疇。由於這樣的法規設計缺陷，臺灣政府將其監管範圍擴展到同時經營廣告業務的網路服務提供者所提供之非廣告業務。這種過度擴張使法遵之範圍變得難以理解且令人困惑，並且缺乏對這些義務的合理解釋。廣告內容或活動的性質、受詐騙濫用之風險與危害，以及其在言論自由理論中之價值，與其他非廣告內容（包括用戶生成內容，user-generated contents，下稱 UGCs）和用戶活動完全不同。前揭義務包括：
 - a. 第 32 條 第 1 項第 2 款要求 IAPs 對涉及詐欺用戶帳號暫停提供服務。這些帳號不一定是「廣告客戶帳號」，也可能是其他非廣告服務帳號，如該條條文和立法說明所示。
 - b. 第 33 條要求 IAPs 下架「內容」，包括如立法說明中明確指涉之非廣告內容，如 UGCs（一般使用者創作內容）。
 - c. 第 38 條要求 IAPs 及其他服務提供者保留用戶和交易資料（不一定是與廣告相關的資料），並在接到臺灣警察、檢察官或法院通知後三天內提供所調取資料。這些資料調取請求不一定伴隨法院核發之搜索票。
2. 本條例要求 IAPs 驗證廣告主（委託刊播者）和廣告出資者身分，適用於所有類型的廣告（第 32 條第 2 項第 1 款）。雖然詳細之驗證程序及標準將由數位發展部事後規定，但依目前草案條文和立法說明已經闡述應以數位簽章、FIDO 或現場查驗作為潛在之驗證程序，這對廣告業務營運來說是一個非常嚴格且昂貴的要求。然而本條例並未給予 IAPs 開發和實施這些程序的寬限期。因為廣告行業所有參與者皆無法立即遵守，也不知如何遵守這些要求，倉促立法並實施相關規範必然會導致市場混亂。

3. 本條例還要求

IAPs

在接到警察通知後對涉詐用戶帳號暫停提供服務，這包括廣告服務和非廣告服務的帳號（第 32 條第 2 項第 2 款）。雖然本聯盟理解通知及暫停程序之時效需求，但此程序並非經臺灣法院審查，且欠缺明確用戶向警察提出救濟之程序。

4. 本條例進一步要求

IAPs

在受主管機關（即數位發展部）或警察通知時，移除與詐欺犯罪相關之內容，包括 UGCs（一般使用者創作內容）。儘管這一要求並未直接對平臺施加罰則，但此條文使臺灣政府能夠在沒有法院審查的情況下、透過對 IAPs 施壓而移除和審查任意之數位內容，恐引發侵犯言論自由之疑慮。

5. 本條例要求

IAPs

及其他服務提供者保留用戶和交易資料（不一定是與廣告相關的資料），並在接到臺灣警察、檢察官或法院通知後三天內提供所調取資料。這些用戶資料調取請求不一定伴隨法院核發之搜索票。這些服務提供者還需要在提交後至少保留調取之資料至少六個月（第 38 條）。這些條文有以下四個問題。首先，所涉及之資料範圍廣泛且未確定。其次，這些調取請求不一定經法院審查，也不伴隨法院核發之搜索票；缺乏法院程序保障之所以有問題，是因為這些用戶資料調取請求本身係侵犯用戶隱私之作為，應以適當之法院審查制衡。這種缺乏保障的情況在不同司法管轄權之間造成了法遵困境（例如依日本法律規範，任何資料若與企業提供的個別通訊密切相關時應視為通訊秘密，受日本國憲法和電信事業法之保護，禁止電信/網路企業在沒有法院令狀的情況下提交相關資料）。第三，接到通知後三天內提交所調取資料，對大多數服務提供者，無分規模大小、本地境外，在操作上不具可行性。最後，在提供資料後進一步保留至少六個月於理殊有未合，因法院、檢察官和警察早已收到所調資料，而仔細保存並確保所獲證據之整全性是國家責任，而非服務提供者之責任，蓋犯罪偵查、起訴和審判係國家所獨有之高權。

6. 該條例通過要求受指定之境外

IAPs

指定在地法律代表，進而創造了臺灣對該類業者直接的法律管轄權，且使上述要求對外國 IAPs 具有強制性，並在不同司法管轄權間創造了不可解消的法律衝突。

7. 該條例還賦予臺灣政府於符合下列狀況時，對被指定之 IAPs 單方面實施「流量管理」（即通過 CDN 降低流量速度）、終止 DNS 解析和「訪問限制」（即通過 DNS RPZ 或其他方法完全阻斷服務）的權力：(a) IAPs 未能指定本地法律代表；(b) 當本地法律代表未能通知或協助受指定之境外 IAPs 法遵時（此情境可能包含任何的法遵錯誤）；(c) IAPs 未能下架違法廣告；或 (d) IAPs

未能暫停提供涉詐用戶帳號服務。這種管制設計雖然援引了臺灣就兒少或成人私密影像相關之法律，但沒有提供任何有意義正當化理由（例如比例原則），而僅僅作為一種強制業者法遵的措施。這種管制設計不僅直接違反臺灣政府允諾「自由和開放網路」的原則，實質上亦形成了一種危險的立法趨勢，進一步偏離和拆解自由與開放網路原則，使其在臺灣變得毫無意義。

8. 法案規定互联网接入提供商（IAPs）对因响应广告而产生的损害承担连带责任。这项规定应当审查其比例性，并确保主要责任在广告商身上。责任不应扩展到与广告商没有合同关系的各方。

9. 最後，雖然臺灣政府聲稱在各種貿易條約和協議中，包括《臺美 21 世紀貿易倡議》，將遵守良好法規實務（GRPs），但臺灣政府未能於此次法規制定過程中遵循

GRPs。本條例草案並未翻譯成英文以便於外國業者理解，未對公眾開放評論，也未在提交予立法院之前邀請各方利益相關者提供意見。這些義務違反嚴重阻礙網路產業的參與、阻礙公民社會的討論，但臺灣政府對此未提供任何解釋。雖然臺灣政府主張詐欺高度嚴重、急迫，以及打擊詐欺是高度社會共識——

這些理由任何網路業的參與者都不會反對的，但此種空泛主張並未詳細說明為何政策急迫性應導致臺灣政府放棄 GRPs，也未能有意義地解釋為何不遵守 GRPs 可以制定良善法律，從而保障人權，併使產業利益與正當程序所實現之依法行政相均衡。