

**Asia Internet Coalition (AIC) Comments on Draft Report of Telecommunications Business
Governance Study Group, Japan**

23 August 2022

Ministry of Internal Affairs and Communications
Telecommunications Bureau
Business Policy Division
1-2 Kasumigaseki 2-chome, Chiyoda-ku, Tokyo, 100-8926, Japan

**Subject: Asia Internet Coalition (AIC) Comments on Draft Report of Telecommunications
Business Governance Study Group, Japan**

On behalf of [the Asia Internet Coalition \(AIC\)](#) and its members, I am writing to express our sincere gratitude to the Ministry of Internal Affairs and Communications (MIC) for allowing us to submit comments on the [Draft Report of Telecommunications Business Governance Study Group](#) (電気通信事業ガバナンス検討会 特定利用者情報の適正な取扱いに関する WG). As an introduction, AIC is an industry association of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. AIC has previously submitted [several policy positions](#) to the key agencies in Japan including the MIC.

As such, please find appended to this letter detailed comments and recommendations (both in English and Japanese - 日本語), which we would like the MIC to consider.

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 our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490.

Thank you



Sincerely,
Jeff Paine
Managing Director, Asia Internet Coalition (AIC)

***Please note that the final comments are submitted in Japanese and the English is provided for review purposes only.**

Proposal Filer	Organization's name	Asia Internet Coalition
	Name of Representative	Jeff Paine
	Contact	Name : Sarthak Luthra TEL : +65 8739 1490 e-mail : Secretariat@aicasia.org

Japanese

該当箇所	意見
2. 特定利用者情報の適正な取扱いに関する規律 2.1 特定利用者情報を適正に取り扱うべき電気通信事業者 (3)対応の方向性	潜在的な負担を最小限にするため、アカウントベースでカウントすることも認めるべきである。また、実数をカウントせず、閾値を超える旨のみを通知することも認めるべきである。ソーシャルメディアやメッセージングサービスごとにユーザー数を算出することを明確化すべき。
2.3 媒介相当電気通信役務 (3)対応の方向性	特定利用者情報の重要性は、事業規模や事業が無料で提供されているかどうかとは関係ない。したがって、閾値はどちらかに統一すべきである。
2.7 情報取扱方針 (3)対応の方向性	政府又は研究会は、日本人が一部の問題国による外国の諜報活動に曝されることを懸念しているようであるが、そのような国が、どうして民間企業に対して、素直的にに情報を求めるのでしょうか。このような検討されて

該当箇所	意見
	いる要求は、無駄な作業を発生させるだけであり、かえって社会的な敵対勢力と戦うための私企業と国家との正当な協力を妨げることになる。
同上	5のような要件は、グローバルな観点からは例外的であり、今後、外交上又は相互主義の観点から、はたまたテロ対策業務において、他国との無用なトラブルを引き起こすことにつながる。 そもそも、情報取扱規程は、企業のプライバシー保護への取り組みを伝えるためのものであり、このような事実を列記することは、情報取扱規程の本質から外れるものである。 もし、総務省がこの要件を維持するのであれば、外務省や警察庁など関係省庁と調整する必要がある。
2.8 特定利用者情報の取扱状況の評価 (2) 検討	取扱状況の評価は、組織の内部的な行為であり、その結果は機密であるべきである。政府に情報を出す可能性があることだけでも、思わぬ結果を招くことになる。研究会は、電気通信事業法第166条の「業務」を私企業の自由な活動に対して過度に介入的に解釈しているようであるが、社内的や組織的な行為が含まれると解釈してはならない。
2.10 特定利用者情報の漏えい報告 (3) 対応の方向性	我々は、総務省が、UAE、インドネシア、カンボジア、シンガポール、タイ、中国、チュニジア、ベトナム、香港、ミャンマー、ラオス、ロシア(以下、「指定国」という。))の当局に対して、企業が日本の顧客及び利用者に関する情報を開示する場合には、総務省への報告を義務付ける提案を検討していると理解している。この提案の目的は、日本の個人情報保護委員会の評価に基づき、国際標準に合致した適切な適正手続の保障又は人権保護措置を確保しない可能性のある法制度から日本国民のプライバシーと安全を守ることであると理解している。

該当箇所	意見
	現在の提案は、報告の範囲が限定される余地が定められていないという点、法律によって要求されているという点、加えて、安全に対する差し迫った脅威を防ぐために必要な状況に対する例外を含んでいないという点から、あまりにも広範に及ぶことを深刻に懸念している。 1. <u>法律の抵触の可能性</u> 総務省に報告を行うことは、指定国の秘密保持法や守秘義務に違反する可能性が高いため、場合によっては、指定国の企業やその社員が捜査、起訴、罰則さらには前科のつくリスクに曝されることになる。例えば、 1. シンガポールでは、汚職、麻薬取引及びその他の重大犯罪(利益の没収)法(the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act)、テロリズム(資金調達の抑制)法(Terrorism (Suppression of Financing) Act)及び組織犯罪法(Organized Crime Act)は、開示者が捜査中であるか、捜査が行われようとしていることを知りながら、またはそれを疑う合理的な根拠を持っている場合には、特定の開示を禁じています。総務省へ報告を行うことはHKNSL実施規則に基づき犯罪行為を構成することになる可能性が高い。 2. 香港では、警察及び「中華人民共和国香港特別行政区における国家安全保障の確保

該当箇所	意見
	に関する法律」(HKNSL)に基づき権限を行使する公的機関への開示は、機密保持が要求されます(さらに総務省へ報告を行うことはHKNSL実施規則に基づき犯罪行為を構成することになる可能性が高い。))。 2. <u>公共の安全</u> 企業は、以下のことを選択せざるを得ないという不利な立場に置かれることになる。 a. 指定された国の一つでデータを開示し、これらの法の抵触・衝突のリスクに苦慮する。 b. 指定国でのデータ開示を拒否し、法の抵触・衝突を回避する。その結果、当局による人命救助、特に海外にいる日本人の人命救助ができなくなるリスクがある。 3. <u>日本の顧客やユーザーを特定すること</u> 企業は、顧客や利用者の法的管轄を正確に把握することはしていない。そのため、外国政府に対する開示のうち、どの開示が日本の顧客または利用者に関するもので、総務省に報告すべきものかを特定することが困難となる。その結果、総務省への開示が過剰になり、日本以外の顧客や利用者のプライバシーに影響を与える可能性がある。同様の理由で、総務省への開示が過少になり、企業が行政処分を受けるリスクにも曝される。 4. <u>国際法</u> 本件提案は、国際法にもそぐわないし(他の法的管轄において同様の法

該当箇所	意見
	律があることを我々は承知していない)、国家主権に対する重大な侵害をもたらすものである。実際、日本の当局はしばしば、法的要請の存在を開示しないよう企業に要求する(刑事訴訟法第197条第5項)。欧州連合の標準契約条項でさえ、法律で許可された場合にデータ対象者に通知する「最善の努力」をすることだけを企業に求めており、EUやその加盟国に通知することを企業に求めてはいないのである。 5. <u>プライバシー</u> また、総務省に開示することで、顧客・ユーザーのデータが2カ国の当局に2度開示されることになり、顧客・ユーザーのプライバシーが侵害されるケースもあります。 これらの理由から、我々は総務省が本件提案を追求しないことを推奨する。上記にもかかわらず、総務省が本件提案を追求するつもりであるならば、我々は以下の場合には総務省への通知が必要ないものとするを強く推奨する。 a. 顧客及び利用者の国籍・居住地が不明である場合 b. 顧客及び利用者が、開示が行われる可能性があることを事前に通知されている場合 c. 開示が有効な法的手続きに対応するものである場合 d. 死亡又は重大な身体的危害の危険があるため、遅滞なく開示する必要があるという誠実な信念に基づいて開示される場合、及び

該当箇所	意見
	e. 総務省に通知することにより、開示しようとする企業にとって重大な法的リスクが生じる場合
同上	検討会は、通信の秘密に係る法的論理が、特定利用者情報の観点にも同様に適用される理由を示していない。すなわち、検討会は、プライバシーポリシーへの利用者の同意に基づき特定利用者情報を提供するかたちで外国政府に協力する場合であっても、それが「漏洩」に該当する理由を示していない。
同上	日本法の令状や捜査関係事項照会書に相当するものに対する開示は該当しないと考える。そもそも、日本と諸外国では法文が全く一致するものではないので、細かな差異がある場合まで組み入れられる余地があるような提案について、明確に反対する。 そのような必要な捜査に関する事項まで「漏えい」と位置付けることは、外国の主権との関係でも問題。 外国主権との関係も考えれば、外国政府の令状等に基づく適正な捜査の場合に違法性が阻却されないとは考えられない。
同上	注47の個情法の関係のところで、個情法上明確に外国における第三者（政府の可能性含む）への提供に有効な個別同意を得ている場合には、電気通信事業法上も有効な同意があるものとして違法性阻却されるとの理解でよい。仮に違法性阻却されないと考えるのであれば、違法性阻却されない理由も明確化して教示されたい。

English

Related part	Comment
2. Rules on the proper handling of specified user information 2.1 Telecommunications businesses that should handle specified user information properly (3) Direction of regulatory response	To minimize the potential burden, it should be permitted to count on an account base. Further, it should also be permitted to notify to the effect that the number exceeds the threshold without counting the actual number. The regulations should clarify that users should be calculated for each distinct social media and messaging service.
2.3 Telecommunications services equivalent to intermediary of communication. (3) Direction of regulatory response	The importance of SUI is not related to the size of business and whether it is for free or not. Therefore, the thresholds should be unified to one of the two.
2.7 Information Handling Policy (3) Direction of regulatory response	It seems that the Government or PSSG is concerned that Japanese people can be exposed to foreign espionage activities by a part of problematic countries. How come such problematic countries ask private sector companies to seek information straightforwardly? This requirement will fail in causing unnecessary tasks only, and prevent legitimate cooperation to fight against social enemies.
Same as above	The requirement like 5 is exceptional from a global perspective, which leads to causing unnecessary troubles in diplomacy/reciprocity and counter-terrorism operations in the future. In the first place, the list of such cases is absolutely inconsistent with the nature of a policy which delivers a company's commitment to privacy protection. If MIC keeps this requirement, MIC should align itself with the Ministry of Foreign Affairs and National Police Agency and related government ministries and agencies.

Related part	Comment
2.8 Evaluation of the status of handling of specified user information (2) Examination	Internal assessment should be confidential. Even producing information to the Government would cause unexpected results. The term “business” here should not be interpreted as including internal and organizational practices.
2.10 Reporting a Leak of Specified User Information (3) Direction of regulatory trend	We understand that the Ministry of Information and Communications (“MIC”) is considering a proposal to require companies to notify MIC when they disclose information about a Japanese customer or user to authorities in the following countries: the UAE, Indonesia, Cambodia, Singapore, Thailand, China, Tunisia, Vietnam, Hong Kong, Myanmar, Laos, and Russia (which we will refer to as the ‘designated countries’). We understand that the goal of the proposal is to protect the privacy and safety of Japanese citizens from statutory regimes which, in the assessment of the Japanese Personal Information Protection Committee, may not provide adequate due process or human rights safeguards consistent with international standards. We are seriously concerned that the current proposal sweeps too broadly because it contains no exceptions for circumstances in which disclosure is limited in scope, required by law, or necessary to prevent an imminent threat to safety. 1. <u>Potential conflict of laws</u>: In some cases, notifying MIC would put companies and their personnel in the designated countries at risk of investigation, prosecution and penalties, often criminal, because disclosure to MIC would likely amount to violations of secrecy laws and

Related part	Comment
	confidentiality obligations in the designated countries. For example,: 1. In Singapore, the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, Terrorism (Suppression of Financing) Act, and Organized Crime Act prohibit certain disclosures when the disclosing person knows or has reasonable grounds to suspect that an investigation is being, or is about to be, conducted (a further disclosure to the MIC would likely constitute a criminal offense);. 2. In Hong Kong, a disclosure to the police and authorized officers exercising powers under the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (HKNSL) is required to be kept confidential (a further disclosure to the MIC would likely constitute a criminal offense under the HKNSL Implementing Rules). 2. <u>Public safety</u>: Companies would be put in the invidious position of having to elect whether to: 1. disclose data in one of the designated countries and grapple with these conflict of law risks; or 2. decline to disclose data in the designated country to avoid conflict of these laws, at the risk of preventing authorities

Related part	Comment
	from taking steps to save lives, and in particular the lives of Japanese personnel who are abroad. 2. <u>Identifying Japanese customers or users</u>: Companies rarely know the jurisdiction of their customers or users with certainty. This will make it difficult for them to identify which disclosures to foreign governments relate to Japanese customers or users and should be reported to MIC. This could result in over disclosure to MIC, impacting the privacy of non-Japanese customers or users. For the same reason, there is also a risk of under disclosure to MIC, which could expose companies to administrative penalties. 3. <u>International law</u>: The proposal is also out of step with international law (we are not aware of a similar law in any other jurisdiction) and presents a significant incursion on state sovereignty— an incursion that Japan itself would not accept if roles were reversed. Indeed, Japanese authorities often demand that companies refrain from disclosing the existence of legal requests (Art. 197, para. 5 of the Code for the Criminal Procedure). Even the European Union’s Standard Contractual Clauses require companies only to make “best efforts” to notify the data subject when permitted by law; they do not require companies to notify the EU or any of its member states. 4. <u>Privacy</u>: In other cases, disclosure to MIC would invade the privacy of the companies’ customers/users by requiring their data to be disclosed

Related part	Comment
	twice to authorities in two different countries. For these reasons, we recommend MIC does not pursue this proposal. If MIC intends to pursue this proposal despite the foregoing, we strongly encourage MIC notification to MIC is not required if: a. the citizenship/residency of the customer or user is not known; b. the customer/user has been given prior notice that disclosure may occur; c. disclosure is responsive to valid legal process; d. disclosure is made pursuant to a good faith belief that a danger of death or serious bodily harm requires disclosure without delay; or e. notification to MIC would create a serious risk of liability for the disclosing entity.
Same as above	MIC does not show the reason why the same legal logic in SoC also applies in terms of SUI. In other words, MIC shows no reason why it constitutes 'leakage,' even when we cooperate with a foreign government by providing SUI based on users' consent to PP/DP.
Same as above	We do not believe that disclosure of information equivalent to a warrant or investigation-related inquiry form under Japanese law to be applicable. In the first place, Japan and other countries do not have the same legal text at all. It is also problematic in relation to the sovereignty of foreign countries to regard

Related part	Comment
	matters related to such necessary investigations as "leakage." Considering the relationship with foreign sovereign countries, it is unthinkable that illegality cannot be denied in the case of a proper investigation based on a warrant issued by a foreign government.
Same as above	Regarding the part about personal information protection law in footnote 47, if individual consent has been obtained to provide information to a third party in a foreign country (including the possibility that this third party is a government agency), we would like you to clarify whether valid consent has been obtained under the Telecommunications Business Act and that it would not be considered illegal. If it would be considered illegal, we would like you to clarify the reason for this.