13 November 2017

Respectfully to: Ministry of Public Security

National Assembly Law Committee

NA Committee for National Defence and Security

National Defense and Security Department, Office of Government

Ministry of Information and Communications

Ministry of Industry and Trade

Attention: Senior Lieutenant General To Lam
The Minister, MOPS

Mr. Ngo Trung Thanh
Member of National Assembly, Standing Member of the National Assembly Law Committee

Mr. Vo Trong Viet
Chairman of the NA Committee for National Defence and Security

Mr. Can Van Lai
Director of National Defense and Security Department, Office of Government

Mr. Nguyen Thanh Hung
Deputy Minister of Information
and Communications

Mr. Cao Quoc Hung
Deputy Minister of Industry and
Trade

Comments on amendments to the Draft Law on Cybersecurity

We write further to our letters of 5th September and 4th August in which we were able to submit comments on the Draft Law of Cybersecurity. We were also pleased to be able to attend the Consultative Workshop on the Draft Law on Cybersecurity in Hanoi on 9th October. We congratulate the Vietnamese Government for engaging in such consultation and welcoming comments from Industry.

Whilst we are very pleased that some amendments have been made to the Draft Law, it is a shame that key areas of concerns mentioned in AIC's first letter still exist in version 14.

Many of our areas of concern, including the Data Localisation requirements and Content Provisions, we submit will have a negative impact on economic & innovation growth and undermine Vietnam's FDI reputation, and Vietnam's ability to achieve Vietnam 4.0 Industry. We urge Vietnam to consider their position very cautiously, as the law as it stands could have huge repercussions for Vietnamese Businesses, general public, and Vietnam's GDP.

Further, we understand that Vietnam is hoping to sign and become a member of TPP. We wish to highlight that the TPP specifically forbids Data Localisation Policies as part of its Electronic Commerce Chapter, instead requires an open internet with free-flowing data.

Areas of concern

1. The scope of the Draft Law is too broad and there are overlaps with existing laws.

We maintain our previous comments that the Draft Law goes significantly beyond the usual cybersecurity laws coverage and steps into internet content controls. In its submission on the Cybersecurity Draft Law, the MOPS notes that the Draft Law is necessary "to assure conformity with international practices," citing examples of cybersecurity Laws in different countries. In these countries, however, cybersecurity is generally limited to maintaining the security of network and information systems. We respectfully refer you to our letter dated 4th August citing examples of other Cybersecurity Legislation. In summary, should Vietnam include provisions such as content controls and data localisation, they are not conforming with International Practices and are therefore not achieving their goal. Indeed, the inclusion of content regulation clauses (which as discussed below, are largely covered by existing

regulations) threatens to draw away much needed attention from the need to address cybersecurity in its traditional formulation.

Further, the inclusion of content regulation is unnecessary as there are other Laws regulating content and the draft contains overlap with content regulation in these existing laws. It may not be necessary to introduce new content restrictions under the Draft Bill, as the Draft Bill covers a narrower scope and provides vaguer procedures for handling illegal information, but also create regulatory uncertainty and inconsistency, as there will be multiple agencies policing content.

Currently, handling of illegal content on the Internet is regulated under Decree No. 72. Cooperation between offshore providers of public information and Vietnamese authority on handing illegal information is currently regulated under Circular No. 38. The basis to identify infringing content that is subject to takedown requests under Circular No. 38 is Article 5.1 of Decree No. 72.

Although some provisions overlap with Decree 72, the draft covers a broad range of prohibited content, including obscene, against honour or dignity of any individual, distorts or defame government officials, propaganda against the country (Sections 8, 22, 34).

Service providers/information system owners are required to corporate with and undertake request from authority to prevent, suspend and delete of prohibited content. Content that is considered false or slanderous information shall be deleted within 24 hours (Section 47). The Draft Law should recognize that websites, web portals or social networks host content that are posted by their users, and thus would not be able to control what the users post. There should be a clear legal process for addressing this issue that, consistent with international practices, should include judicial oversight in respect of requests for content removal.

We affirm that the inclusion of this list of prohibited acts confuses and dilutes the stated objective of cybersecurity. The use of cybersecurity legislation for censorship and reporting of those censored, the Law appears to allow cybersecurity legislation to be used as a reason for blocking and filtering of content. Globally, cybersecurity does not include this type of activity, and we submit there is no place for content control in Cybersecurity Legislation.

2. The Bill imposes onerous measures and liabilities on internet service providers that would potentially impede the digital economy and the growth of internet services in Vietnam.

As set out below, Article 8 (2) (Prohibited Acts) includes "Posts, or dissemination of information contents on cyberspace that are fabricated, distorted, embarrassing, slanderous, or offending in respect of the prestige of any organisation or the honour or dignity of any individual". As we have previously stated, platforms do not have the physical ability to monitor every post and decide whether or not it complies with the law. Further, they do not believe it is their place to do so. Even if they had the capability and desire to do so, the content limitations are so broad and vague that to do so would be impossible. We respectfully remind the Vietnamese Government that whilst we always believe improvements can be made, all our member companies have policies regarding many of these types of content, and will voluntarily remove them if the content is found to be in breach.

Article 34 (3) states "Telecommunication and internet service enterprises and enterprises possession information systems shall set up their mechanisms to authenticate information when users register digital accounts to assure the confidentiality and the honesty of registration information…". Article 47 covers the responsibilities of telecommunication and internet service corporate providers and 47 (1) (a) states "require the users to provide their authentic information".

As previously submitted, there is no viable way for companies to do this. They simply have to trust that their users are providing accurate information as they have no means of checking it. However, companies have policies regarding what to do if a user has signed up in breach of their policies, for example if they discover an underage child has registered.

Article 34 (4) states that "Foreign enterprises, when providing telecommunication and/or internet services in Vietnam shall compel with Vietnamese legislation, respect the national sovereignty, interests and security of Vietnam, obtain licenses for their operations, locate their representative offices and services in which Vietnamese users data are administered in the territory of the Socialist Republic of Vietnam, secure user information and users account information and sanction violations stringently under legislation".

The provisions above are also very relevant to our concern below that it will increase the difficulty and cost of doing business in Vietnam. We submit that these requirements will impede both the digital economy and the growth of internet services in Vietnam, making it less competitive and less of an attractive investment for FDI.

Article 47 (dd) states "Not to provide telecommunication, internet, technical support, advertisement, or payment support services to any organisations or individuals that post information containing any content against the State of the Socialist Republic of Vietnam, false, or slanderous information on cyberspace". We understand the intention behind this provision, however we submit it is too broad and lacking in clarity. In theory, a user could

post a review of something accidentally calling it by the wrong name or misspelling the name. According to this provision, in theory, the website where that is posted would not be able to accept any advertising or payments. This surely cannot be the outcome that Vietnamese Government would think appropriate.

3. The Bill will increase the difficulty and cost of doing business in Vietnam.

We submit that the increased difficulty and costs of doing business in Vietnam as a result of this legislation will not only deter new entrants to the Vietnamese market (both foreign and local) but could result in existing companies withdrawing their services in Vietnam entirely. This could potentially have a huge impact on Vietnamese small businesses, many of whom rely on services offered by foreign internet companies to export their goods.

Article 34 (4) (quoted above) and Article 48 (4) quoted below both contain data localization and local office requirements.

Because of the broad definition of "information systems critical to the national security" under Article 9, Article 48 (4) potentially covers many providers that offers services using the Internet.

Article 48 (4) states "When collecting or creating **personal information and critical data, to store the same within the country**. Where it is obligatory to provide any information out of the country, to assess security levels as regulated by the Ministry of Public Security or in accordance with legislation where it provides for this*."*

There are extensive reasons why the free flow of data helps the country's economy (and conversely, how localization requirements will discourage business development). The Data Localisation Requirements in the Draft Law will cause significant impact on SMB's as well as larger companies. The AIC website has three reports which outline the damage that data localisation policies can do and the benefits of free flowing data.

We respectfully highlight that it is not only foreign companies who will be affected by data localisation policies, in fact smaller companies are more likely to be Vietnamese and the cost for smaller businesses will be proportionately higher than for larger companies. As set out in the ECIPE report, the effect of Data Localisation is not simply that it will affect businesses, it will also affect GDP. According to the World Economic Forum, "the flow of digital information between countries, companies and citizens is increasingly recognized as a critical driver of economic growth and innovation, particularly in the age of the knowledge economy." At a time when Vietnam is looking to conduct an IT Law Review to benefit from the digital economy and promote Vietnam 4.0, data localisation policies should be avoided

for the private sector. Companies should be allowed to choose the best option for their company regardless of location.

Locating data servers locally does not increase cybersecurity for data and it can be counterintuitive as cybercriminals can more easily identify the location of the data for cyberattacks since the search zone is now narrowed down to data servers within a country (as opposed to letting companies decide globally where to locate their or their customers' data). An effective cybersecurity strategy is one where there is good execution of ever-evolving best practices in security to the combined areas of technology, processes, people and physical facilities.

Companies have made huge investments to ensure that their data centres are secure. Forcing companies to locate servers locally would make them more vulnerable to attack as the systems and network might be less sophisticated, and generally harder to update with the latest security software. We strongly suggest any data localisation requirement be limited to only Government information systems. Further, The TPP's electronic commerce chapter expressly forbids data localisation, requiring members to embrace an open internet. Should Vietnam sign the TPP as it desires, it would need to remove any data localisation requirements in domestic legislation.

We also maintain that the requirement to set up a local office may result in Vietnamese people being deprived of digital services, or having to pay more for these services, as these burdens become too onerous or costly.

4. Vague appraisal procedures in relation to products and services used in Critical Systems may be inconsistent with WTO commitments

Our previous comments here remain relevant, and are set out below. As this area of concern is around international commitments, we yet again remind the Vietnamese Government of its commitment to the free flow of data in the TPP Electronic Commerce Chapter, and strongly urge them to reconsider their approach of data localisation.

Article 20.2(b) of the Draft Law requires that products and services intended to be used in Critical Systems be reviewed/appraised by the competent agency under the MOPS or by a professional organization authorized by the MOPS. However, the Draft Law contains no detail on any review / appraisal procedures, as well as on any objective criteria to establish whether a specific product or service is fit for use in Critical Systems. Vague review / appraisal procedures may result in non-transparent procurement procedures and discrimination between offshore suppliers and domestic suppliers. Additionally, the application of vague appraisal procedures may constitute unnecessary technical barriers to trade or domestic regulations which are inconsistent with Vietnam's WTO commitments.

5. Breaches of the law may to criminal proceedings and persecution

Depending on how different articles of the Draft Bill are combined and interpreted by the enforcement authority, breaches (or suspected breaches) of the law may still be subject to criminal proceedings and persecution. As stated in our previous letter, we submit criminal penalties should be removed from the draft law.

Article 6 contains a list of Cybersecurity Protection Measures, for example Article 6 (h) Prevention and suspension of the provision of cyber information in an area for a period when there is any sign of harm to national defence and security. Article 6 (i) Prevention of any illegal transmission, deletion or change of, or access to, information in cyberspace. Article 6 (m) Suspension of operations when there is a ground to determine that an activity in cyberspace has a sign of harm to national security; temporary suspension or required stop of operations or revocation of domain names in respect of information systems in accordance with laws. Article 6 (o) Prosecution, investigations, application of restraining orders, forced measures or discovery ones in accordance with the laws on criminal proceedings. Article 6 (2) he Government shall provide in detail the sequence, procedures, and authority to apply cybersecurity protection measures.

Article 8 contains Prohibited Acts. Article 8 (1) contains a large list of prohibited actions including " The use of cyberspace to oppose the State of the Socialist Republic of Vietnam; prejudice national security or social order and safety, sabotage great national unity; propagate an aggressive war or terrorism, cause enmities or conflicts between nations or religions; incite sex or racial discrimination; propagate or instigate violence, cause violent disturbances, disrupt security to disturb public order; post embarrassing slanderous obscene depraved or felony information; practise prostitution or social evils or traffic in human; sabotage the fine customs and practices of the nation, social morality of public health".

Article 8 (2) posts, or dissemination of information contents on cyberspace that are fabricated, distorted, embarrassing, slanderous, or offending in respect of the prestige of any organisation of the honour of dignity of any individual". Further, Article 34 (1) states "any use of cyberspace to perform any act in violation of legislation shall be severely sanctioned".

The coverage in Article 6 and Article 8 is very broad and is beyond the arena of national security. It also shows some overlap with other legislation such as law on advertising. Without interpretive rules, vague texts such as 'honour and dignity of the individual' may present threats to Internet service providers over Internet content. Specifically, Article 8 entitles state authorities to demand Internet service providers to remove content or to apply penalty measures including withdrawing licenses under

Article 22.

The combination of Article 8, Article 6 and Article 34, make it unclear as to whether criminal penalties remain within the act, and if so what they are. We submit that when it comes to criminal liabilities, there is no room for vague statements and the law should specify very clearly whether or not criminal liability applies, if so provide an appropriate level of detail. As we have previously submitted, we do not feel that this Act is the appropriate place for content control, and neither should criminal penalties apply. We believe that the Vietnamese Government did intend to remove criminal liabilities from the Draft Law, but we would like to see drafting amendments so that this is clear.

Additionally, Article 11 (3) states that "the Ministry of Public Security shall verify capacity and conditions in respect of corporate providers of cyber information safety services for information critical to national security.

Article 11 (4) states The Ministry of Public Security shall introduce detail provisions on cybersecurity verification with respect of the information systems critical to the national security,".

The previous version attributes this function to the Government, and we submit that it should remain with the Government.

6. Lack of clarity including clear definitions

Article 3 covers the interpretation and definitions. However, In Version 14, many definitions are omitted, in fact no definitions have been added despite comments on the lack of clarity. there are still no definitions in the Draft Bill for telecommunications and internet service providers. As both "Telco service provider" and "Internet service provider" services require both a local presence and data localisation as set out in Article 34, they should be clearly defined. As previously suggested, for a definition of telecommunications provider, we would welcome a definition similar to "telecommunications carriers" in the US (that is, only internet service providers).

As previously commented, the Draft Law again does not conform to international standards as it does not use standard definitions of cyber security, and instead conflates cybersecurity with data protection and criminal use of the internet, for example, for terrorism or speech against the state. There is a consistent lack of clarity throughout the Law. It appears that the Law covers everyone using the internet and any organisation, but definitions lack clarity. For example, we remain unclear as to the meaning of 'information systems of the information industry and sector'? (Art 18).

Our previous comments, set out below, remain relevant:

The Draft Law would require information system owners to coordinate with government cybersecurity agencies to identify the origin of cyberattacks perpetrated on the owners' systems as set out in Article 12 & 4. Additionally, if the government declares that there is an increased risk of an "urgent circumstance as to cybersecurity," the Ministry of Public Security (MOPS) may require organizations to "collect and report related information in a timely fashion" and to coordinate with the agency to prevent an attack. Art. 16 §§ 1(a), 3. We recommend the Vietnamese Government limit the application of this provision to circumstances in which a cyberattack creates a risk of harm for users. We further suggest that it would be helpful for the term "related information" to be defined, in order that there is transparency and no accusations can be made that the Government is using this provision to extract unrelated information.

The Draft Law would deem certain information systems to be "critical to the national security," including those that are used in State-sponsored industries, those "affecting the national sovereignty, interests, and security," and those "seriously affecting the social order and safety," among others (referred to herein as "Critical Systems") as set out in Article 18 & 1. MOPS would have the authority to establish cybersecurity standards for Critical Systems and to audit them, including by analysing data derived from the systems and related documents, and to implement "technical solutions and professional operations" for any perceived deficiencies, as set out in Articles 20-21. Critical Systems operators would also be responsible for reporting any cybersecurity incidents and working with MOPS to remedy them, and MOPS would have the power to halt the Systems' operations during remediation, as set out in Article 22. We propose that Critical Systems be re-defined to include only systems that are part of the state-sponsored national infrastructure.

The Draft Law would require organizations to remedy "any security error or flaw" found in a "cyber product or service," and to notify users and authorities of any such flaws, as set out in Article 31 & 1(d). "Cyber products and services" are defined broadly to include "hardware, equipment and software, catering for the operations of cyberspace, or stored or transmitted thereon." We request that the Vietnamese Government limit this definition to security errors or flaws that are known to have compromised user security and that voluntary reporting is the most appropriate way to ensure appropriate transparency. We also seek to clarify that there is no requirement to reveal the exact nature of the flaw, as publicizing every security flaw could tip off criminals to new attack vectors.

7. Restrictions on Civil Liberties and extent of prohibited acts

We re-iterate our earlier points, set out below.

The Draft Law includes a very broad range of prohibited acts, including:

- The use of cyberspace to prejudice the national sovereignty, interests and security, or the social order and safety.
- Posts on cyberspace against the State of the Socialist Republic of Vietnam, prejudicial to the legitimate rights and interests of organisations or individuals, or contrary to the morality or the fine customs and practices.
- Unauthorized intrusions on or appropriations of information or documents.
- Cyberattacks.
- Cyberterrorism.

In addition to our concerns raised about the broadness and vagueness of this definition and its impact upon the digital economy in Vietnam as set out in Point 2 above, it seems that Article 8 holds 'any organisation violating the Law' responsible whilst Articles 9 and 10 allow the Vietnamese Government to 'temporarily suspend, suspend, or withdraw the operating licence of, the website or the web portal posting the information' of any individual calling on:

- 'people to join a mass gathering that disturbs the security and order';
- posting information that is:
- distorting a historical truth, negating a revolution achievement, or sabotaging the great national unity;
- distorting or defaming the people's government;
- being any fabrication or causing any confusion among the people;
- causing a psychological warfare, inciting an aggressive war, or causing enmities between nations and the people of countries;
- propagating reactionary thoughts;
- offending the nation, a famous person or national hero;
- fabricating, spreading or dispersing what are clearly known to be false to offend human dignity or honour, or to embarrass or slander any organisation or individual;
- instructing or inciting any acts in violation of legislation;
- prejudicial to the legitimate rights and interests of any organisation or individual, or contrary to the morality or the fine customs and practices on cyberspace.

The inclusion of this list of prohibited acts confuses and dilutes the stated objective of cybersecurity. The use of cybersecurity legislation for censorship and reporting of those

censored, the Law appears to allow cybersecurity legislation to be used as a reason for blocking and filtering of content. Globally, cybersecurity does not include this type of activity.

The Draft Law advocates 'cyber security supervision' (Section 3) and 'licensing' (Section 4) which could be argued is akin to industrial espionage, and may require companies to register and receive certification to provide cyber security advice to users. Such a requirement will reduce the security of Any globally legitimate cybersecurity Law should have no role in this type of activity.

The Draft Law would prohibit “the use of cyberspace” to engage in certain types of speech, including speech that “prejudices the national sovereignty, interests and security, or the social or and safety,” and “posts on cyberspace” that are against Vietnam’s government or “contrary to the morality or the fine customs and practices” (referred to herein as “Prohibited Speech”) and as set out in Article 7 & 1-2. The Draft provides examples of Prohibited Speech, including “distorting or defaming the people’s government,” “causing confusion among the people,” and “offending the nation, a famous person or national hero,” among other categories, as set out in Article 10 & 2. It further states that organizations and individuals may not “produce, post, store, or disperse” the Prohibited Speech Articles 10 & 4.

We respectfully suggest you consider limiting the definition of “cyberspace” to only public internet channels on the grounds that it is not feasible for companies to monitor the content of messaging sessions, etc., even if a company had the technical capability to do so. We further seek to more narrowly define the categories of prohibited speech to include only concrete threats, such as terrorism, threats of violence, etc. This will assist in the perception of this Law as a genuine Law for security and not for control of content.

Further, with regard to mandatory cooperation with authorities to combat “mass gatherings disturbing the security and order” the Draft Law requires “telecommunications providers” (a term not defined in the Law) to “closely coordinate with the competent authorities in handling the information on cyberspace that incites mass gatherings disturbing the security and order.” As set out in Articles 9 & 3. We again propose that you consider limiting the definition of “telecommunications provider” to a definition similar to “telecommunications carriers” in the US (that is, only internet service providers).

The Draft Law would require telecommunication service providers to put in place “technical measures to prevent the displaying of, and delete,” the Prohibited Speech, as set out in Article 10 & 5. We recommend that Vietnam limit the filtering requirement only to publicly-available communications, on the basis that private communications between just one or a handful of people are unlikely to incite the undesired behaviour.

Summary

We once again congratulate the Vietnamese Government for its efforts in legislating this complex but vital area of Law. We do hope that our comments give the Vietnamese Government an insight into the industry perspective, and we will be more than happy to provide further comments or answer any further questions the Vietnamese Government may have. We urge the Government to very carefully consider their International commitments, and the negative effect some aspects of this policy could have on the people, businesses, reputation, FDI and GDP of Vietnam.

Yours sincerely

Jeff Paine

Managing Director

Asia Internet Coalition