20 February 2018

Respectfully to: Ministry of Public Security

National Assembly Law Committee

National Assembly Committee for National Defence and Security

National Defence and Security Department, Office of Government

Ministry of Information and Communications

Attention: Senior Lieutenant General To Lam

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

Comments on amendments to the Draft Law on Cybersecurity – Version 15

Introductory Remarks

We wanted to express thanks for the opportunity to provide further comments on Vietnam's draft cyber security law. We would like to continue to congratulate the Vietnamese government on addressing cybersecurity issues, and including in your strategy resources and training, support for a cybersecurity industry, and support for research.

We appreciate, as industry, how important protecting cyber security is. We think this is a shared challenge, and it is crucial that government, industry and civil society stakeholders work together to tackle the shared challenges of online security in Vietnam. Our companies would like assure you that we will actively contribute to the security of our products, as used by Vietnam's citizens.

We believe in addition to focused cybersecurity legislation, industry should work more proactively with the Vietnamese government providing training and engagement throughout Vietnam on cybersecurity issues. Our companies would like to provide a renewed effort to programmes, product and business initiatives necessary to ensure the security of internet users throughout Vietnam.

In particular our members would like to share their expertise on security by design, talking through their four pronged approach: (i) providing tools and education to users to allow them to protect themselves; (ii) ensuring strong security is built into products, utilizing, where appropriate internationally recognized security; (iii) developing a strong cybersecurity ecosystem, for example by creating and sharing open source software; and (iv) internal auditing and reporting mechanisms.

Whilst we support, in general, the cybersecurity efforts highlighted by the draft law, we have concerns about the non-cybersecurity issues the draft law also seeks to address, in particular issues of national security. The draft includes a number of measures beyond protecting key local infrastructure - such as intermediary liability for a variety of content types, data localisation and child safety. These issues, especially national security, are all important and we want to make clear our collective commitment as industry to mitigating the harms from online services, and maximising the benefits to people, governments and the economy. This includes providing effective channels for the flagging of locally illegal content. However, we do not believe that cybersecurity legislation is the place to address these issues.

We believe the blending of cybersecurity with national security and other non-relevant issues creates obligations that will harm local Vietnamese businesses, make it extraordinarily difficult for non-Vietnamese businesses to operate and actually prevent industry from proactively pursuing solutions to the shared concerns of cybersecurity. We would therefore be grateful if, in addition to engaging on cybersecurity programmes, we could continue engagement on the law.

Article 27. Cyber information security

1. Organisations and individuals shall be responsible to respect and strictly implement legislation on cybersecurity, and act in cyberspace in line with the behavioural rules; any use of cyberspace to perform any act in violation of legislation shall be severely sanctioned.

2. Websites, web portals or specialized pages on social networks of agencies, organisations and individuals shall post information in accordance with legislation, and shall not provide, post or transmit information with any content prejudicial to national sovereignty and security.

3. Telecommunication or internet service enterprises and enterprises possessing information systems shall set up their mechanisms to authenticate information when users register digital accounts to assure the confidentiality of registration information, and shall provide such information to relevant specialized force in charge of cybersecurity protection when required. The registrants of such digital accounts shall be responsible to protect and use the accounts they create in accordance with legislation.

4. Foreign enterprises, when providing telecommunication and/or internet services in Vietnam, shall:

a) comply with Vietnamese legislation, respect the national sovereignty, interests and security of Vietnam;

b) locate their head offices or representative offices in the territory of Vietnam when having 10,000 or more Vietnamese users or when required by the Government of the Socialist Republic of Vietnam;

c) store in Vietnam Vietnamese users' data and other important data that are collected or produced from using the national cyberspace infrastructure of Vietnam, in the case stated in Sub-Article 27.4(b) above;

d) secure user information and users' account information;

dd) implement requirements from the competent authorities of Vietnam in preventing or removing any information contents that are prejudicial to national security, social order and safety or the legitimate rights and interests of organisations and individuals; provide Vietnamese users' data and sanction violations of legislation on cybersecurity.

Data Localisation (Article 27 4 c and Article 42 (4))

We note the changes made with regard to data, and that the local data server provisions have been removed and replaced with local data storage of local user data and other important data. However, while the new provisions allow for local data storage in third

party providers' services (instead requiring companies to own servers in Vietnam), this still prevents the free flow of data between borders. We submit that there are both economic and technical reasons why this provision should be removed, and data should be allowed to flow freely. Data localisation inhibits the functionality and smooth running of global technology platforms. In practice, international technology platforms rely on global cloud infrastructure to deliver consistent services, and it is generally not possible or practicable to neatly segregate cloud based data by jurisdiction.

Legal reasons to allow Free Flowing Data

We would like to highlight to the Vietnamese Government that the electronic commerce chapter in the TPP prevents data localization — as a prerequisite for conducting business. If Vietnam wishes to join the TPP, the data localization contained in this law will be in breach of the agreement.

Economic reasons to allow Free Flowing Data

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 SMBs 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 strongly recommend that the Vietnamese Government considers the ECIPE Paper "THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ECONOMIC RECOVERY" which states that if Vietnam were to legislate for Data Localisation, its GDP could reduce by 1.7%, a 3.1% decrease in investment and a $1.5 Billion USD of welfare losses. The report states "As this study has shown, this impact is a direct consequence of the complex relations between cross-border data flows, supply chain fragmentation and domestic prices. These are complexities that are generally not understood by policymakers, who are often in the field of security and privacy law, rather than international trade. The findings regarding the effects on GDP, investments and welfare from data localisation requirements and discriminatory privacy and security laws are too considerable to be ignored in policy design. It is also reasonable to assume that SMEs and new firms are the first to be displaced from the market, as they lack resources to adapt to the regulatory changes".

According to Ed Brzytwa, in his article "Let the Data Flow: Why Eliminating Data Localization Requirements Can Only Benefit the Global Economy" "The global economy depends on the free movement of data". He explains "Governments that enact data localization policies often cite two primary reasons for doing so: 1) they believe that local mandates will benefit their countries' economies; and 2) they assert it is to protect the privacy and security of their citizens' data and personal information. They are generally not aware, however, that

data localization requirements can lead to adverse outcomes and do not accomplish either of these goals."

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.

Technical reasons to allow Free Flowing Data

In the article "Where Is Your Data, Really?: The Technical Case Against Data Localization" by Dillon Reisman, the complexities of storing data are explained. It is a complex matter, but essentially, data can be in many different places in part or in whole, and sometimes in more than one place at a time. This, along with regular backups, ensure that data is never actually lost. However, if data is only stored in one place, it is susceptible to being lost as a result of human error, a natural disaster or other complication.

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.

Local Office Requirements (Article 27 4 b)

We note that the local office requirement has changed to “head office or local representative office” requirement. We highlight that the local representative office does not serve the authorities’ intended purpose as the representative office is not an authorized entity to provide any user data and has no decision making authority for content removals. This requirement along with the data localisation requirement 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. We do not believe that the requirement for tech companies to establish a physical presence in Vietnam is necessary to address Vietnam's cybersecurity - or content removal - concerns, which can be addressed remotely. Companies without a presence - for legitimate business reasons - will find themselves non-compliant with Vietnamese law. This will make it more difficult for smaller start ups to provide services in Vietnam. Further, this law will make it harder for these businesses to grow in Vietnam in the future. Similar requirements by other countries will have an impact on Vietnamese start ups.

Prohibited Acts (Article 8)

1. The use of cyberspace to oppose the State of the Socialist Republic of Vietnam; prejudice national security, social order and safety or the legitimate rights and interests of organisations and individuals; sabotage great national unity; incite an aggressive war or terrorism; cause enmities or conflicts between nations; propagate or instigate violence, cause violent disturbances, disrupt security or disturb public order.

2. The use of cyberspace to offend any religion or for sex or racial discrimination; post 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 or public health.

3. Posts or dissemination of information contents on cyberspace that distort the history, negate a revolution achievement, or offend the nation or a national hero, or that are fabricated, distorted, embarrassing, slanderous or offending in respect of the prestige of any organisation or the honour or dignity of any individual, or guide how to carry out a terrorist attack.

4. The use of cyberspace to propagate, link or induce other persons to join any organisations, societies or groups against the Party or the State; organise, train or drill other persons to oppose the Party or the State; and to communicate, advertise, purchase or sell any of such goods or services as are specified in the prohibited list under legislation.

5. Conducting cyberattacks, cyberterrorism, cyberespionage, or sabotaging, attacking or encroaching on any information systems critical to national security.

6. Producing or putting into use any tools, means or software or having any acts that obstruct or disorder the operation of any computer network or telecommunication network; spreading any computer program that is malicious to the operation of any computer network, telecommunication network or electronic means; or unauthorized intrusion into any other persons' computer network, telecommunication network or electronic means;

7. Taking advantage of or abusing cybersecurity protection to prejudice national sovereignty, interests or security, social order and safety or the legitimate rights and interests of any organisations or individuals, or for private gain.

8. Taking any acts on cyberspace in violation of this Law or any other laws.

We have strong concerns around the Government's use of the law to outlaw broad categories of online speech and expression. These prohibitions are more consistent with other criminal offences rather than factual concerns about cybersecurity, and may also lead to accusations of censorship. While we also appreciate that the Government's concern to move swiftly against events as they emerge, the takedown procedures outlined in the law are also inconsistent. The law requires offending content be taken down within 24 hours, however there lacks clarity on whether this procedure is intended to cover all of restricted content.

We re-iterate our previous comments on this point. Current regulations, primarily Decree No. 72/2013/ND-CP, sets out what are deemed to be prohibited acts in relation to the provision and use of internet services. The list of prohibited acts under this decree already suffers from overbreadth and vagueness, and has been the subject of (see http://www.asiainternetcoalition.org/aic-comments-on-vietnams-Draftinternet-decree-on-internet-services-and-online-information/). This Draft Law does little to address the uncertainties brought about by Decree No. 72, and instead contains even broader and vaguer provisions as to what constitutes prohibited content.

This uncertainty and the potential liabilities imposed on internet service providers would tend to dampen innovation in the provision of internet services and, on a wider scale, the growth of the digital economy in Vietnam.

We re-iterate our earlier comments 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 allows cybersecurity legislation to be used as a reason for blocking and filtering of content. Globally, cybersecurity does not include this type of activity. 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. Terms such as "social morality" in Article 8(2) are too broad and open to interpretation.

Article 41. The responsibilities of telecommunication and internet service corporate providers

1. In performing cybersecurity protection activities

a) To require the users to provide their authentic information.

b) To develop plans and solutions to rapidly respond to any cybersecurity incidents and immediately remedy security risks such as security flaws, malicious codes, cyberattacks or cyber intrusions; on the occurrence of any cybersecurity incident, to immediately implement an emergency plan and appropriate responses and, at the same time, to report the same to their governing agencies according to regulations.

c) To cooperate with, to provide technical measures and support to, the public security bodies during their criminal investigations and protection of national security under legislation.

d) To apply technical solutions and other necessary measures to assure safety and security in collecting information and preventing any possible data revelation, leakage, damage or loss. If any revelation, leakage, damage or loss of user information data occurs or is likely to occur, to immediately put in place response solutions, at the same time to give notices to the users and to report the same to their governing agencies in accordance with regulations.

dd) To coordinate with specialized forces in charge of cybersecurity protection in, and facilitate, their cybersecurity protection.

2. In assuring cyber information safety

a) To keep confidential, store and use their users' personal information under legislation, and at the same time to develop and consolidate their personal information protection policies.

b) Not to disclose, change or provide any information to any third party without the prior consent of the information owner.

c) To update, revise, delete or correct any information collected illegally as required by the user;

d) To prevent the sharing of information, to delete information containing any content against the State of the Socialist Republic of Vietnam, false or slanderous information on the telecommunication or internet services provided by them within 24 hours as from the time as required by the specialized force in charge of cybersecurity protection, and at the same time to keep related records for report to such specialized force;

dd) 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;

e) To develop and consolidate cybersecurity protection processes and cooperation mechanisms, to increase the assessment and analysis of cybersecurity risks, to give periodic warnings of dangers, and at the same time support and assist other members in enhancing their responsiveness to cybersecurity risks;

g) To develop their feedback or complaint mechanisms in respect of cyber information safety; to disclose information on their feedback or complaint methods; in a timely fashion to receive and deal with feedbacks or complaints in respect of cyber information safety;

h) To undertake any requirements from the competent authorities under the Ministry of Public Security, the Ministry of National Defence and the Ministry of Information and Communications in investigating and dealing with violations of law in cyberspace.

3. The Government shall detail the sanctioning of violations by telecommunication and internet service corporate providers of the provisions on cybersecurity protection.

Firstly, we note that "telecommunication and internet service corporate providers" is not defined in the act. As per our previous comments, we would ask that "telecommunications provider and internet service corporate providers" be defined similarly to "telecommunications carriers" in the US (that is, only internet service providers).

We respectfully ask how the Vietnamese Government would like our members to comply with Article 41 (1) (a) – notably "To require the users to provide their authentic information"? Companies rely on their users providing accurate information. However, accounts are closed down in the event that it becomes apparent that false data has been provided.

With regard to Article 41 (2) (d):

d) To prevent the sharing of information, to delete information containing any content against the State of the Socialist Republic of Vietnam, false or slanderous information on the telecommunication or internet services provided by them within 24 hours as from the time as required by the specialized force in charge of cybersecurity protection, and at the same time to keep related records for report to such specialized force;

We ask the Vietnamese Government to 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 – i.e obtain a court order.

Over-broad cyber security requirements: in order to be successful, the technology

ecosystem requires a flexible approach to address the cybersecurity concerns of the future as well as the present: As global leaders, our members face the challenge of maximizing the benefits of technological progress while minimizing the harms, including cybersecurity threats. We have concerns that the requirements to prevent and eliminate cyber attacks, identify the origins, block or filter information that the government states is part of a cyber attack and follow broad instructions issues by the government are overly broad. Cybersecurity threats and responses evolve rapidly, so prescriptive regulations would likely be quickly outdated and, worse, counter-productive.

Concluding Remarks

Many of the goals of this legislation are worthwhile and important. We want to work with you to ensure that the practical compliance requirements set out in the law for businesses (both based in Vietnam and internationally) are both clear and not disproportionately onerous. Legislative confusion will make it harder for companies to both operate in Vietnam, and provide industry-led solutions to shared challenges.

We also hope that continued work on cybersecurity and content removal - areas of common interest - can compliment the legislative measures. As industry, we'd be delighted to meet to discuss these issues in further detail. Please do not hesitate to reach out to us.

Yours sincerely

Jeff Paine, Managing Director

Asia Internet Coalition


ASIA
INTERNET
COALITION