22 Jul 2013

Mr. Vu Quoc Khanh (vqkhanh@mic.gov.vn)
Director, Vietnam Computer Emergency Response Team – VNCERT
Ministry of Information and Communications, Vietnam

Dear Mr. Vu,

Re: Vietnam's Draft "Law on Information Security," version 2.22, issued on May 22, 2013

The Asia Internet Coalition (AIC) is an industry association formed by eBay, Facebook, Google, and Yahoo! Incorporated. We seek to promote the understanding and resolution of Internet policy issues in the Asia Pacific region.

We appreciate the opportunity to provide comments on Vietnam's Draft Law on Information Security. Security is fundamental to ensuring that Internet users have a good experience online and that their personal information is protected.

Since technology evolves very rapidly, we suggest that the law avoids being overly prescriptive in order to allow flexibility by companies and by the Government. We suggest, where possible, to limit prescriptive measures to Government systems and critical infrastructure so that private companies are able to continue innovating.

For the law to be enforceable and for companies to have certainty in complying with the law, it is important to be explicit about what is allowed and what is prohibited. Articles that are overly broad should either be clarified or removed.

While AIC companies are happy to work with the Government of Vietnam to address issues like spam and malware, we are concerned that the law may attempt to apply extraterritorially. Foreign companies will be reluctant to cooperate on security matters with the Government of Vietnam if the Law applies extraterritorially. We suggest the Government limit the scope of the law to domestic companies.

We submit the following specific comments for your consideration. We would be most willing to work with Vietnam on Internet-related issues and provide views where appropriate. Should you have any further queries please do not hesitate to contact director@asiainternetcoalition.org for any further information on the contents of this submission.

Thank you.

Best wishes,

Dr John Ure
Executive Director
Asia Internet Coalition

Asia Internet Coalition's Comments on Vietnam's Draft Law on Information Security, 18 Jul 2013

Article 2
This article is overly broad and should be clarified. It is unclear at what stage the law applies to a foreign individual or organization.

Article 4
These definitions contained in this section are very broad, and we request that they be defined very specifically, in order to avoid confusion. Some examples include:

- The definition of "information security infringement" uses the "unauthorized" construct that has proven itself to be problematic because what constitutes authorization in a networked and often autonomous computing environment is not always easy to establish.
- The term "unauthorized" is also problematic as there is no element of intent.
- The definition of "malware" also lacks an intent element.
- The definition of "personal information" seems vague and difficult to apply because of the lack of specificity.
- It is unclear what is meant by "crypto" in the definition of "civic crypto" but given that this area is highly regulated later in the statute, "crypto" needs more specificity.
- The definitions of "information weapon" and "information conflict" are unclear and could have a very broad interpretation. The current definition confuses the network *system* and the *content*. We recommend a clearer delineation between the two definitions.

Article 5
Principle 2 contains a requirement to notify the authorities of incidents without any attempt to distinguish insignificant events from significant events. We would also request for clarification on how to go about the reporting process (Article 5.2). Principle 4 mandates "cooperation" with the State without clarifying the requirements for "cooperation".

Article 8
This article is circular because it sets forth what is illegal by reference to doing things "illegally" - a term that is not defined.

- Article 8.1 - It is unclear what is meant by: "mislead information on the internet".
- Article 8.4 - The article should make clear that intent is required for these activities to be considered illegal. For example, if a user is not aware that they are spreading spam or malware, they should not be held illegal. "Spam" should also be defined. Unclear definitions in this article could limit free expression online.
- Articles 8.5 and 8.6 - These articles are overly broad and should be clarified. Terms like "obscene" are very subjective and have the potential to be misused to restrict legitimate forms of expression.
- Article 8.6 - Internet service providers merely provide a platform for their services and should not be held responsible for individual user generated content. In order to allow new innovative services to continue to be developed and made available, safe harbour provisions are necessary to exempt platform providers from liability if the platform providers have programs to process legitimate law enforcement requests.

Article 10
This article lacks specifics but implies the desire by the Government to heavily regulate the industry, which will likely lead to the enacting of regulations that are too prescriptive and don't move at the speed of technological innovation.

Article 11 and 13
These article appears to be giving very broad monitoring authority to the Government which would place undue requirements onto public service officers, and should be limited to the extent possible. In addition, it may have the unintended effect of limiting entrepreneurship and freedom of expression. Additionally, it is unclear if Article 11.4 is intended to apply to foreign service providers.

Article 14
This article seems to apply to all information and all possessors of information in Vietnam (40 million Internet users and growing). As such, the requirement is extremely broad, and how to classify information "according to importance level of information and subject to access" is not detailed enough to be implemented. This would also place a large burden on individual users and small businesses, and is likely to be a barrier to foreign investment in Internet services in Vietnam as it would entail extra compliance costs. This article should be clarified.

Article 15
This article seems similar to the US CAN-SPAM Act of 2003, but is very vague and lacks specifics. Article 15.3 - This article should be clarified to clarify which service providers are covered by this article. Many service providers are intermediaries and as third parties, would not be able to control the content they transmit over their networks.

Article 16.2
We would request the process for incident reporting to be referenced and clearly communicated.

Article 18
This article mandates email providers report incidents of malware to authorities. This requirement is unusual, and it is difficult to assess the extent of the reporting (e.g. should individual consumer incidents be reported?) We recommend that it be removed.

Article 19
- 19.1 – we request more clarification on "provide adequate information" and "coordinate with state competent management".
- 19.5 - Given the definition of malware is so broad, this Article would be nearly impossible to implement and comply with, and could lead to abuse.
- Article 19.1.d Internet service providers merely provide a platform for their services and should not be held responsible for individual user generated content. In order to allow new innovative services to continue to be developed and made available, safe harbour provisions are necessary to exempt platform providers from liability if the platform providers have programs to process legitimate law enforcement requests.

Article 20
This article is very broad and should be clarified.
- Article 20.1 - This article is very broad and too prescriptive. The article seems to apply to any user who has a "computer crash." For example, if a user needs to restart their computer, it appears they are legally required to provide notification.
- Article 20.2 - "Information safety activities" isn't defined, but the responsibilities of organizations engaged in such activities include very broad activities such as not "putting negative impact on politics, economy and culture" and seems to require management and inspection by government authorities.

Articles 21-23
The purpose of these articles is unclear.

- Article 21.2 – many service providers facilitate communications between third parties, and are unable to know or control the content they transmit. “Risk” assessment should also be clarified.
- Articles 22.4 - This article is overbroad and has the potential to be applied to legitimate online expression.
- Article 23.2 - This article is overbroad and implies that organizations, including online intermediaries, have a legal obligation to prevent the spread of “false information”. This article is impossible to implement and comply with.
- Article 23.3 - The meaning and intent of this article is very unclear and could lead to abuse, and limiting of freedom of speech online.

Article 24
This article does not define "terrorist purposes" and has could be used to restrict legitimate online expression. This article also seems to give broad powers to government given "terrorist purposes" isn't defined.

Article 25
This article again makes it illegal to do things that are "illegal” without defining what is “illegal”. There is no explanation of how citizens or providers should enforce “prevention” of illegal activity”.

- Articles 25.1 & 25.2 seem redundant of prior sections (and similarly lacking in an intent element).
- Articles 25.3 & 25.4 seem very broad and potentially create intermediary liability. It is important that intermediaries not be held liable for third party content.
- We recommend that Vietnam explore the Budapest Convention on Cybercrime as to draft an article which specifically discusses cybersecurity measures for the country.

Article 26
“Personal information” and “personal needs” are not defined clearly.

Article 27
This article gives broad protections for "personal information" without any exceptions.

- For example, exceptions are required to comply with the law.
- Many sub-principles could be improved by clarify the parameters for consumer consent, collecting, using, updating, removing and sharing consumer data. We suggest an article to be focused on personal privacy data law, that specifies the

Article 28
This article does set forth any structure for users to make such demands or for companies to comply with them. Circumstances for requiring requests for personal information should be defined.

Article 30-38
Crypto is not fully defined, but should be clear not to cover encryption.

- This article seems to be going down the path of government mandating standards, which usually ends up hindering innovation. It would be better if such mandates only applied to government entities and critical infrastructure.
- The sub-principles refer to the public and commercial use of crypto, but commercial use of cryptography includes common IT devices and services, such as in VoIP calls, using a secure company phone, or even logging into a secure WiFi network. We recommend providing clarity, else there is the risk of too much burden being placed on IT companies and individuals to do reporting (Article 32.1, 33.2), or to safeguard their interests (Article 33.3, Article 3).
- Article 32.1, 33.1 – we recommend clarifying “specific origin”.