Vietnam's cyber-security law strengthens privacy… a bit

Christian Schaefer, Managing Partner, Asia Counsel, Ho Chi Minh City, Vietnam
Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2016) 141 *Privacy Laws & Business International Report*, 26-27

Vietnam's new *Law on Cyber-Information Security*, enacted in November 2015,[1] comes into effect on 1 July 2016 (the "Law"). As a law enacted by the National Assembly, it is the second highest form of legislation in Vietnam, superseded only by Vietnam's Constitution and international treaties.[2] This article assesses whether the Law's scope, and the data privacy principles it sets out, significantly expand Vietnam's existing data privacy laws, which to date are, in a piece meal manner, scattered across various regulations that apply to the IT, telecommunications, banking, e-commerce and consumer privacy sectors.[3] Section references are to the Law except where noted.

Clearer concept

The Law provides clearer concepts of personal information and processing, but with a focus limited to commercial processing and only in cyberspace. It offers two useful definitions for personal information and data processing. It provides that '[p]ersonal information means information associated with the identification of a specific person' (Art. 3(15)) and '[o]wner of personal information means a person identified based on such information' (Art. 3(16)). This is a broader definition of 'personal information', especially when compared to existing definitions in Decree 72/2013/ND-CP on the Management of Internet Use where 'personal information' is defined as 'information which is attached to the identification of the identity and personal details of an individual including name, age, address, people's identity card number, telephone number, email address and other information as stipulated by law' (Article 3(15) of Decree 72) or Decree 52/2013/ND-CP on E-commerce where personal information is defined as 'information contributing to identifying a particular individual, including his/her name, age, home address, phone number, medical information, account number, information on personal payment transactions and other information that the individual wishes to keep confidential.' (Article 3 of Decree 52). The broader scope of the definition is significant as the Law spells out prohibited acts in relation to processing personal information.

Furthermore, and unlike the Law on Information Technology which does not define 'processing' of personal information, the Law now defines '[p]rocessing of personal information' as 'the performance of one or some operations of collecting, editing, utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purposes' (Art. 3(17)). Articles 17 to 19 of the Law then provide comprehensive regulations on requirement how personal information must be managed. However, the definition at the same time limits the scope solely to 'organisations and individuals processing personal information' in a commercial context and does not apply to the processing of personal information for government or non-commercial purposes. In addition, given the overall ambit of the Law, the Law imposes these requirements only to processing of personal information in cyberspace.

---

[1] *Law on Cyberinformation Security,* National Assembly, No. 86/2015/QH13, November 19, 2015.

[2] G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), p. 363.

[3] Greenleaf *Asian Data Privacy Laws* Chapter 13 'Vietnam and Indonesia – ASEAN's Sectoral Laws'.

The law is unusual in that it defines 'cyberspace' to mean 'an environment where information is provided, transmitted, collected, processed, stored and exchanged over telecommunications networks and computer networks' (Art. 3(2)). This suggests that the scope also includes VPNs and possibly certain intranets. 'Information system means a combination of hardware, software and databases established to serve the creation, provision, transmission, collection, processing, storage and exchange of information on the network' (Art. 3(3)), and the scope of the Law is thus limited to cyber-information security activities on such network.

Cyber-security with a privacy balance

'Cyber-information security means the protection of information and information systems in cyberspace from being illegally accessed, utilized, disclosed, interrupted, altered or sabotaged in order to ensure the integrity, confidentiality and usability of information' (Art. 3(1)). Article 4 sets out the general obligations of organisations (private and public sector) and individuals to ensure this cyber-security, but also requires that '[t]he response to cyber-information security incidents must guarantee lawful rights and interests of organizations and individuals and may not infringe upon privacy, personal and family secrets of individuals and private information of organizations' (Art. 4(3)). Security should therefore not trump privacy.

A code for data privacy in cyberspace

Within this limited scope, Chapter II Section 2 of the Law sets out what is probably the most comprehensive set of data privacy principles yet found in a Vietnamese law (Arts. 16-19). Without significantly departing from previous laws, the following requirements imposed on organisations and individuals that process personal information within a commercial context are more precise:

- *Consent requirements* – 'Collect personal information only after obtaining the consent of its owners regarding the scope and purpose of collection and use of such information' (Art .17(1) (a)).
- *Use limitation* – 'Use the collected personal information for purposes other than the initial one only after obtaining the consent of its owners' (Art. 17(1) (b)).
- *Disclosure limitation* – 'Refrain from providing, sharing or spreading to a third party personal information they have collected, accessed or controlled, unless they obtain the consent of the owners of such personal information or at the request of competent state agencies' (Art. 17(1) (c)). The State need only 'request', so there is no effective limitation on disclosure by state agencies.
- *Right of access* – 'Owners of personal information may request [processors] to provide their personal information collected and stored by the latter' (Art. 17(3)).
- *Automatic deletion and notification* – '… shall delete the stored personal information when they have accomplished their use purposes or the storage time has expired and notify such to the owners of such personal information, unless otherwise prescribed by law' (Art. 18(3)).
- *Publication of protection measures* – '…shall develop and publish their own measures to process and protect personal information' (Art.16(3)).

Enforcement

'Prohibited acts' in cyberspace include not only spreading spam or malware but also '[i]llegally collecting, utilizing, spreading or trading in personal information of others; abusing weaknesses of information systems to collect or exploit personal information' (Art. 7(5)) which is broader in scope and encompasses illegal acts of third parties more comprehensively than the prohibited acts set out currently in the Law on Information and Technology. Moreover, hacking 'information on clients that lawfully use civil cryptographic products' (Art.

7(6)) is prohibited. But 'using or trading in civil cryptographic products of unclear origin' is also prohibited (Art. 7(6)), so privacy protection via cryptography is of limited legality in Vietnam. Trading in 'civil cryptographic products and services' must be licenced (Chapter III, Civil Cryptography), and can be suspended at the request of state agencies (Art. 35(6)).

'Individuals violating this Law shall, depending on the nature and severity of their violations, be disciplined, administratively sanctioned or examined for penal liability and, if causing damage, pay compensation in accordance with law' (Art. 8). Unlike the Law on Information and Technology that sets out different consequences for violations by individuals and organisations, it is unclear what the sanctions for the violations committed by organisations are under the Law until implementing regulations provide more details on consequences for violations by organisations.

Article 20 requires only of 'state management agencies' to 'establish online information channels for receiving petitions and reports from the public' and to 'annually inspect and examine personal information-processing organizations and individuals; to conduct extraordinary inspection and examination when necessary'. It would seem that they are then able to take enforcement steps under Article 8.

The Ministry of Information and Communications has the most general responsibility for implementation of the Law (Art. 52(2)), including '[t]o conduct examinations and inspections, settle complaints and denunciations, and handle violations of the law', but other specified Ministries also have significant responsibilities (Art. 52(2)(h)).

Conclusion: Another sectoral law for Vietnam

From a privacy perspective, this law is therefore limited to 'commercial processing of personal information in cyberspace'. The existing Vietnamese data privacy laws are sectoral laws, and the Law has not introduced any major changes to the existing regulations. However, the content of the data privacy protections is generally more precise and stronger. It is to be seen whether the implementing regulations of the Law will provide any further development. So far, it is another small step forward.

Authors: Christian Schaefer is Managing Partner at Asia Counsel, Ho Chi Minh City. Email: christian@asia-counsel.com.

Graham Greenleaf is Asia-Pacific Editor for Privacy Laws & Business International Report.