Vietnam's 2013 e-commerce Decree consolidates data privacy protections

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales

Privacy Laws & Business International Report, Issue 125, 22-24, September 2013

For the past eight years, Vietnam has steadily expanded and strengthened its legislative protections of privacy in relation to e-commerce, and in consumer transactions generally. Government Decree 52 of May 16, 2013 on e-commerce[1], which took effect on July 1, 2013, replacing a previous Decree,[2] is Vietnam's most detailed data privacy regulation so far.

Vietnam is still a one party state, theoretically socialist but with a thriving private sector operating beside state-owned enterprises (accounting for about 40% of GDP). With a population of over 90 million, it is the fourteenth most populous country in world. It has been a WTO member since 2007, and is a negotiating partner in the Trans-Pacific Partnership discussions. Vietnam has an export-oriented economy, and has considerable foreign direct investment running at over $10 billion per annum. Although GDP growth slowed in 2012 it is still growing at around 5% per annum. Vietnam therefore has one of the more significant and growing economies in the ASEAN region and Asia generally. Data privacy laws in the private sector are likely to be of growing significance as it becomes more involved in international trade in goods and services.[3]

The existing e-commerce and consumer laws

Article 38 of Vietnam's *Civil Code*, entitled 'Right to Privacy' provides a brief and general requirement of consent for the collection and publication of information about the private life of a person, and protection of the confidentiality of mail, telephonic and electronic communications. This provision has resulted in litigation, including a court issuing a judgment in 2012 interpreting Article 38 in favour of a company's right to access and monitor an employee's work email account.[4]

IT and e-commerce laws

The systematic development of data privacy laws in Vietnam commenced with its e-commerce laws. The *Law on E-Transactions* of 2005 provided a brief broad statement of an individual's right to consent to the use of their personal information in e-commerce.[5] The 2006 *Law on Information Technology*[6] ('IT law') provided more detailed regulations concerning collection, processing, use, storage and provision of personal information. 'Network environment' is defined to mean 'an environment in which information is supplied, transmitted, collected, processed, stored and exchanged via information infrastructure' (A 4). Where there are 'other laws on the same matters related to information technology application and development activities', the provisions of this law will prevail. The law applies to bodies 'engaged in information technology application and development activities' (A 1). It applies to 'agencies, organizations and individuals' even where they are referred to as 'organizations and individuals', and therefore may apply to public sector

[1] Decree No. 52/2013/ND-CP dated May 16, 2013 of the Government on e-commerce, available (Unofficial translation) at <http://luatminhkhue.vn/copyright/decree-no-52-2013-nd-cp-dated-may-16,-2013-of-the-government-on-e-commerce.aspx>

[2] It supersedes Decree No. 57/2006/ND-CP dated June 9, 2006 of the Government on e-commerce.

[3] For background see 'Vietnam', pgs 180-97 in Church, P (Ed) *A Short History of South East Asia* (5th Ed.) Wiley, 2009 and Hayton, B *Vietnam – Rising Dragon* Yale University Press, 2010. For readily accessible current statistics, the 'Vietnam' pages of both the CIA Factbook and Wikipedia are both useful.

[4] Tran Manh Hung, Seck Yee Chung, and Quach Minh Tri (Baker & McKenzie Vietnam) 'Company's Right To Monitor Employee Emails Affirmed By Court', 21 September 2012, 12 *World Data Protection Report* 31.

[5] Article 46(2) 'Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consent, unless otherwise provided for by law'.

[6] *Law on information technology* (No. 67/2006/QH11), available at <http://www.asianlii.org/vn/legis/laws/oit264/oit264.html >

bodies (A 1), but this would need to be specified in regulations (A 7(5)). It explicitly applies to 'foreign organisations and individuals' carrying out such activities 'in Vietnam' (A 2).

Articles 21 and 22 set out obligations on organisations covered by the law in relation to consent, exceptions for processing without consent, notice, use, retention/deletion, security, access (perhaps), correction (including blocking until corrected), disclosure, and compensation. These obligations cover most of the matters normally found in a data privacy law. Their content is now substantially repeated (often in very similar terms), but also made more detailed, in the 2013 Decree, as discussed below.

The IT Law contains a number of other privacy-protective provisions. The anti-spam provision includes an obligation to ensure that where consumers provide notice that they do not wish to receive 'advertisement information' that wish is observed (A 70(3)), and to assure their 'ability to reject' such advertisements (A 70(2)). Using false names to send information is also prohibited (A 70(1)). Article 70 constitutes a direct marketing opt-out protection. The prohibition on those who 'create, install or spread computer viruses or harmful software' specifically refers to the purposes of 'collecting other people's information' and 'modifying or deleting information' (A 71). Article 72, in addition to a very general obligation to protect confidentiality of personal information,[7] prohibits a range of activities (most types of 'computer crime') including a 'catch all' prohibition of acts which endanger individuals' information[8].

Consumer Protection Law

The 2010 *Law on Protection of Consumers' Rights*[9] (the 'Consumer Law') took effect on July 1, 2011, replacing the 1999 *Ordinance on Protection of Consumers Rights*. Its provisions strengthen consumers' rights, including those on the use, collection and transfer of consumer information, in a brief but broad data privacy code. The scope of terms such as 'personal information' and 'consent' is not defined in this law, but other laws shed some light on their meaning. The new law expands those obligations in regard to all consumers, not just in the context of e-transactions (as was the case with earlier laws), but does not change the substance of those obligations.[10]

Business entities 'trading goods and/or services' (including individual traders) will have to satisfy the requirements of Article 6 'Protection of consumer information'. This includes a general confidentiality and security obligation (with a broad exemption for state agencies): 'Consumers' information shall be kept safe and confidential when they participate in transactions, use of goods or services, except where competent state agencies required the information'. It also includes five more specific obligations concerning the collection, use and transfer of consumer information':

> 'a) Notify clearly and openly the consumer of the purpose of the collection and use of consumer information before such activities being done; b) Use information in conformity with the purpose informed to consumers, and with the consent by the consumers; c) Ensure safety, accuracy, completeness during collection, use and transfer of consumer information; d) Update or adjust by themselves or help

---

[7] Article 72(1): 'Organizations' and individuals' lawful personal information which is exchanged, transmitted or stored in the network environment shall be kept confidential in accordance with law'.

[8] Article 72(2)(e): 'Other acts of causing unsafety to, or disclosing confidentiality of, other organizations' or individuals' information which is exchanged, transmitted or stored in the network environment'.

[9] *Law on Protection of Consumer's Rights* of November 17, 2010 at <http://vbqppl.moj.gov.vn/vbpq/en/Lists/Vn%20bn%20php%20lut/View_Detail.aspx?ItemID=10489>

[10] Baker & McKenzie (2011) 'Consumer Protection Law' *Client Alert*, January 2011; Baker & McKenzie (2010) 'Vietnam's New Consumer Protection Law Consolidates Consumer Rights on Protection of Personal Information' *Client Alert*, December 2010.

> consumers to update and adjust as the information is found to be incorrect; e) Only transfer consumer information to third parties upon the consent of consumers, except where otherwise provided by law'.

There are some other provisions in the Consumer Law which could also be valuable for privacy protection (and affect direct marketing), including Article 10 ('Prohibited behaviours') which includes:

> '(1) 'Attempt of organizations or individuals trading goods and/or services in deceiving or misleading consumers via advertising activities, or hide or provide information that is incomplete, false or inaccurate about one of the following details: …c) The contents and characteristics of transaction between consumers and organizations or individuals trading goods and/or services'; and
>
> (2) 'Organizations or individuals trading goods and/or services harasses consumers through the marketing of goods and/or services contrary to the wishes of consumers 02 or more times or other acts that obstruct or affect normal works or activities of consumers'.

The 2013 e-commerce Decree

In summary, the protection of data privacy in Vietnam first occurred through a number of e-commerce, IT and consumer laws enacted by the National Assembly, the highest source of law in Vietnam. The 2013 Decree is made by the Government pursuant to both the IT and Consumer Laws (and other laws), and is what in some other countries would be considered a regulation, although one made by the government as a whole, not one made by a Ministry.

Under the IT law, the Ministry of Post and Telematics has the prime responsibility, but this Decree gives the implementation responsibility to the Ministry of Industry and Trade (MoIT), which is responsible for the Consumer Law. Although Decree 52 therefore seems to state that Industry and Trade now has the responsibility for data privacy in Vietnam (at least in relation to all forms of consumer-oriented business), local experts point out[11] that the new Decree 72 on Internet management imposes the obligation to implement this broader decree on internet management onto the Ministry of Information and Communication (MoIC), and consider that this is likely to spill over into the data privacy aspects of Decree 72 as well. Article 2.2 of Decree 52 requires MoIT to coordinate with MoIC.

Decree 52 defines e-commerce activity broadly, as the conducting of any part of commercial activities 'by electronic means connected to the Internet, mobile telecommunications network or other open networks' (A 3(1)). 'Personal information' is defined as 'the information contributing to identify a specific 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 would like to keep confidential' but 'does not include work contact information and other information that the individual has published himself on mass media' (A 3(13)). Collection of personal information is also defined as 'the collection of information to put it into a database' (A 3(14.)).

The scope of the Decree limits it to those businesses 'involved in e-commerce activity in Vietnam's territory,' including 'foreign individuals residing in Vietnam' and 'foreign traders and organizations with their presence in Vietnam through investment operation, establishment of branches and representative offices or website set-up under Vietnamese domain name' (A 2(1)). So some extra-territorial activities may be subject to the law, but the requirement of 'e-commerce activity in Vietnam's territory' must still be satisfied. Decree 52 grants MoIT and MoIC authority to adopt separate regulations for purely foreign players conducting e-commerce with Vietnamese counter-parties, although local experts note that it is not yet clear when these will be adopted.[12]

---

[11] Email communication from My Doan and Christian Schaefer of Hogan Lovells, Ho Chi Minh City.

[12] Email communication from My Doan and Christian Schaefer of Hogan Lovells, Ho Chi Minh City.

Where a data controller authorises a third party ('processor') to collect personal information, there must be an agreement between the parties specifying which has responsibility for compliance with the various obligations of the Decree, and if they do not then both will be liable (A 68(2)).

One of the 'prohibited acts in e-commerce activities' is 'stealing, using, disclosing, transferring and selling information related to business secrets of other traders, organizations or individuals or personal information of consumers in e-commerce without the consent of the parties concerned, unless otherwise regulated by law' (A 4(4)(a)).

Vietnam's data privacy principles

The 2013 Decree makes the principles set out in Articles 21 and 22 of the IT Law more specific, so references to the Decree are given below (unless the IT Law is specified). However, it should be remembered that the higher source of legal authority is the IT Law. The most important aspects of these principles are now summarised.

Collection and notice

Businesses collecting personal information must publish (or give notice of) their data privacy policies so that it is clearly displayed before or at the time of collection, and if collected through a website is in a conspicuous place (A 69). The data privacy policies must include the purpose of collection; scope of use; duration of storage; who has access; contact details of the unit gathering and managing information; and how consumers can access and modify their personal information (A 69).

Businesses must obtain 'prior consent' to collection of personal information, obtained through a 'mechanism for the information subjects to clearly express their consent through online functions on the website, e-mail, messages or other methods as agreed by the two parties' (A 70). There is no requirement that the information collected must be the minimum necessary for the stated purpose.

Consent is not required for the collection of personal information (a) 'that has been publicized on e-commerce websites'; (b) 'to sign or perform contract of sale and purchase of goods and services'; or (c) to calculate prices and charges for online services (A 70(4)). The extent of the exceptions in (a) and (b) is unclear.

Use, disclosure and transfer

In addition to the requirement of collection by consent, there must also be a 'specific mechanism' for information subjects to permit or refuse (a) 'sharing, disclosure and transfer of information to a third party' or (b) 'using of personal information to send advertisements and introduce products and other commercial information' (A 70(3)). There must therefore be provisions which at least allow consumers to opt-out of direct marketing.

Personal information can only be used (or shared, disclosed or transferred) for the 'purpose and scope announced' except (a) where there is a separate agreement for additional uses; (b) to provide services or products at the request of the information subject; or (c) to perform obligations required by law (A 71).

Security and data breach notification

'The information gathering unit must ensure the safety and security for personal information' (A 72(1)), and some details are specified.

A very limited form of data breach notification requirement is included: 'In case the information system is attacked causing risk of loss of consumer's information, the information storing unit must notify the authorities within 24 hours after the detection of incident.' (A 72(3)). This does not cover

where the security breach is due to system operator's own fault, rather than an 'attack.' There is also no obligation to inform the information subjects affected.

Consumer rights: Access, correction, complaint and deletion

The Decree is quite explicit on these rights, more so than the Laws on which it is based: 'The information subjects have the right to require the information gathering unit to perform the checking, update, modification or deletion of their personal information' (A 73). The IT Law only stated that there was a right to 'request' these matters (A 22, IT Law), whereas here these rights are required (assuming accuracy of translations). The business may either take these steps for the information subject, or 'provide the information for the information subjects to check, update or modify their personal information by themselves' (A 73(2)).

The business must also 'have a mechanism to receive and settle the consumer's complaints concerning the improper use of personal information' (A 72(2)), and the notice given to consumers refers to a 'way of contact for the consumers to ask about the collection and processing information related to them' (A 69(1)(e)), so it is clearly intended that information subjects should be able to query any aspect of how their personal information is processed.

Enforcement provisions

The IT Law states that 'individuals may claim compensation for damage caused by violations in the supply of personal information' (A 22(3), IT Law), but this only refers to supply (disclosure) breaches. However, another provision states generally that businesses 'if causing damage, they shall pay compensations therefor in accordance with law' (A 77, IT Law). The 2013 Decree states in the section concerning 'administrative violations' that businesses 'that violate and cause damage to material interests of … individuals, they must make compensation as prescribed by law' (A 78(3)). It appears therefore that any breaches of the privacy principles can potentially result in a claim for compensation.

The Decree provides that administrative sanctions will apply to 'violation of regulation on protection of personal information in e-commerce' (A 78(1)(h)), and that such sanctions will be handled according to the provisions of the Law on Handling of Administrative Violations (A 78(4)). Various authorities could be involved: 'Inspector of the Ministry of Industry and Trade, the market management agency, inspector of the Service of Trade and Industry of centrally-affiliated provinces and cities and other State agencies have the right to sanction administrative violations in the e-commerce activities under the competence specified in the Law on Handling of Administrative Violations and the relevant documents' (A 78(5)). However, according to the relevant enforcement Circular, complaints about personal information are to be made to MoIT, and can be made online to the Management Portal of e-commerce activities at <www.online.gov.vn>.[13]

Businesses are subject to annual inspection by MoIT (and of equivalent province and city authorities) and are subject to a 'name and shame' provision in that 'result of inspection shall be published in Management Portal of e-commerce activities' (A 77). Once a business receives notice of a complaint from MoIT, it only has ten days to reply before it goes on the 'name and shame' list on the MoIT website, and before administrative sanctions can be brought against it.[14]

---

[13] Article 24(1)(d) and (2), Circular No. 12/2013/TT-BCT dated June 20, 2013 of the Ministry of Industry and Trade promulgating the regulation on notification, registration and information publication procedures related to e-commerce website

[14] Article 24(3), Circular No. 12/2013/TT-BCT dated June 20, 2013 of the Ministry of Industry and Trade promulgating the regulation on notification, registration and information publication procedures related to e-commerce website

The IT Law provides that 'disputing parties are encouraged to settle their disputes over information technology through conciliation; when parties fail to conciliate, their disputes shall be settled in accordance with law' (A 75(2), IT Law), and the Decree reiterates that this applies to e-commerce disputes (A 76(5)(c)), without requiring that conciliation must first occur.

These provisions are all within the context of the IT Law which provides that where there are 'violations of law' (which may be civil or criminal), the responsible parties may be 'disciplined' or 'examined for penal liability' (in the case of individuals), or 'suspended from operation' (in the case of organisations) or 'administratively sanctioned' (in either case) (A 77, IT Law).

Conclusions: Uncertain enforcement of APEC+ principles

Vietnam has enacted data privacy laws in the private sector, although limited to e-commerce (like China) and in somewhat more limited terms, consumer transactions generally (unlike China). The privacy principles that are now made more explicit in the 2013 Decree are a reasonable approximation of the basic principles set out in the OECD Guidelines or the APEC Privacy Framework. On some points, such as deletion rights, direct marketing opt-out and data breach notification, they go slightly beyond those minimal sets of principles. These three provisions are becoming common in other Asian countries, almost to the extent that they can be thought of as 'OECD/APEC+' provisions.

To what extent these rights will be observed by businesses in Vietnam, or enforced by the MoIT or MoIC, or equivalent local authorities, remains to be seen. Some authors such as Sharbaugh are very sceptical about the value of legislative provisions such as the 2006 IT Law, concluding (based on interviews with lawyers in Vietnam) that 'the few existing regulations are obscure and widely ignored'.[15] However, such laws are now being made more precise. Vietnamese citizens, whether acting as consumers or otherwise, are not yet accustomed to using the legal system to enforce their rights, but Vietnamese society is in a process of rapid change and there may be more exercise of consumer rights in future.

My Doan and Christian Schaefer of Hogan Lovells International LLP, Ho Chi Minh City office, have generously provided assistance with the completion of this article. Thanks also to Patrick Sharbaugh for providing a copy of his book chapter. All responsibility for content remains with the author.

[15] Sharbaugh, P 'What's mine is yours: An exploratory study of online personal privacy in the Socialist Republic of Vietnam' in Maj, A (Ed.) *Cyberculture Now: Social and Communication Behaviours on the Web*, Interdisciplinary Press, Oxford UK, 2013.