Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia-Pacific news

Gabriela Kennedy [1,*]

Mayer Brown JSM, Hong Kong

Keywords:
Asia-Pacific
IT/information technology
Communications
Internet
Media
Law

ABSTRACT

This column provides a country by country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

Gabriela Kennedy *(Partner), Mayer Brown JSM* (gabriela.kennedy@mayerbrownjsm.com);

Karen H.F. Lee *(Senior Associate), Mayer Brown JSM* (karen.hf.lee@mayerbrownjsm.com).

1.1. *Signing up to the future – SFC accepts digital signatures*

On 24 October 2016, the SFC released a Circular confirming that digital signatures generated by certain recognised certification authorities outside Hong Kong will be accepted for client identity verification purposes.

1.1.1. *Digital signatures*

Under the Electronics Transaction Ordinance (Cap. 553) ("**ETO**"), electronic signatures and digital signatures are recognised in Hong Kong as having the same legal status as a handwritten signature, so long as certain requirements are met and the transaction is not excluded from the application of the ETO.

The ETO distinguishes between an electronic signature and a digital signature. An electronic signature is defined under the ETO to mean "any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted for the purpose of authenticating or approving the electronic record", e.g. an individual name typed into the signature block of an online form. An electronic signature will satisfy any legal requirement for a signature, so long as certain conditions are met. For example, the method used to attach or associate the electronic signature with an electronic record must be reliable and appropriate.

In contrast, a digital signature is a type of electronic signature, which is supported by a digital certificate that essentially guarantees the identity of the person making the electronic transaction. Such guarantee is provided by a certification authority that issues a digital certificate unique to an individual, and only the individual can use it in order to execute an electronic transaction and the authenticity of the signature in it. For example, an electronic representation of a person's handwritten signature that is generated using that person's private key, which is password protected.

Unlike electronic signatures, digital signatures benefit from a statutory presumption as to their veracity and authenticity,

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.

[1] For further information see: www.mayerbrown.com.

http://dx.doi.org/10.1016/j.clsr.2016.12.005
0267-3649/

so long as the digital signature is supported by certificate issued by a recognised certification authority. In Hong Kong, there are currently 2 recognised certification authorities (the Hong Kong Post Certification Authority of the Postmaster General and the Digi-Sign Certification Services Limited).

1.1.2. *SFC's circular*

Under the Code of Conduct for Persons Licensed by or Registered with the SFC ("**Code of Conduct**"), the SFC sets out guidelines on how a licensed company may verify the identity of a client for anti-money laundering purposes, where the account opening documents are not executed in the presence of the licensed company (e.g. where the client is overseas).

It has always been clear under the Code of Conduct that digital signatures which have been certified by certification authorities recognised by the Hong Kong government are acceptable to the SFC for client verification and account opening purposes. However, it was not clear whether digital signatures supported by a certificate issued by certification authorities outside of Hong Kong, would also be permitted by the SFC under the Code of Conduct.

On 24 October 2016, the SFC released the Advisory Circular to Intermediaries, Client Identity Verification in Account Opening Process ("**Digital Signature Circular**") which now confirms that digital signatures generated by certification authorities outside Hong Kong, whose digital signature certificates have obtained mutual recognition status from the Hong Kong government, will have the same legal status as digital signatures issued by Hong Kong recognised certification authorities.

So far, the Hong Kong government has recognised 3 foreign certification authorities, namely (1) the Guang Dong Certificate Authority Company; (2) the Guangdong Electronic Certification Authority Company Limited; and (3) the Shenzhen Digital Certificate Authority Center Company Limited, pursuant to the Arrangement for Mutual Recognition of Electronic Signature Certificates between Hong Kong and Guangdong Province of the People's Republic of China. This is part of a pilot program being run by Hong Kong and mainland China.

1.1.3. *Conclusion*

The Digital Signature Circular provides further clarity to licensed corporations dealing with clients who are based overseas, but may have little impact in practice given that so far, only 3 overseas certification authorities have been recognised by the Hong Kong government, all of which are based in the Guangdong province of mainland China. Until the Hong Kong government enters into mutual recognition agreements with other countries, licensed companies will not have the comfort of knowing that the digital signatures obtained from customers outside of Hong Kong (or Guangdong) are sufficient under the Code of Conduct.

2. China

Gabriela Kennedy *(Partner), Mayer Brown JSM (*gabriela.kennedy@mayerbrownjsm.com*);*

Xiaoyan Zhang *(Counsel), Mayer Brown JSM (*xiaoyan.zhang@mayerbrownjsm.com*).*

2.1. *China passes cybersecurity law*

On 7 November 2016, the Standing Committee of the National People's Congress of China ("**NPC**") passed the controversial Cybersecurity Law (the "**CSL**"). The CSL has gone through three readings since the release of the first draft on 6 July 2015 and will take effect in June 2017. As China's first comprehensive privacy and security regulation in the cyberspace, the CSL enhances data protection in many aspects while bringing in compliance challenges for the international community at the same time.

2.1.1. *Applicability*

The CSL adopts a tiered approach and imposes different obligations and duties to Critical Information Infrastructures ("**CIIs**") and network operators. "Network operators" are defined to include operators of basic telecommunication networks, Internet information service providers, and key information systems. The definition of "CII" has adopted an earlier version that makes specific reference to a few key sectors such as finance and transportation while retaining the broad catch-all phrase from the second draft to cover "infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, the national welfare, the livelihoods of the people or the public interest." Both the second and third drafts stated that the exact scope of CIIs would be determined separately by the State Council, leaving the government with considerable leeway to bring industries not specifically singled out in the definition into the scope of the legislation at a later stage. Some of the heightened requirements, such as data localisation and cross-border transfer restrictions, apply to CIIs only.

2.1.2. *Data localisation and cross-border transfers*

Under perhaps one of the most controversial provision of the CSL, operators of a "CII" are required to store within China "citizens' personal information and important data" collected or generated during business operations in China. If, for legitimate business reasons, the data must be provided to a foreign entity outside China, the operators must complete a "security assessment" jointly formulated by the National Cyberspace Administration and State Council. Notably, the initial draft applied the localisation requirement to "citizens' personal information and other important data" while the later draft revised this to "citizens' personal information and important data." The second draft also narrowed the scope of data subject to localisation to only data collected or generated within China. While the first draft seemed to allow operators to "store abroad such data or provide it" to an entity or individual located abroad provided that it passes a security assessment, the later draft removed the overseas storage option. The terms "security assessment" and "important data" remain undefined.

Upon a narrow interpretation of this localisation requirement, all Chinese citizens' personal data and transaction data collected or generated within China may be required to be stored in China. This in essence would mean a segregation of the global information system into one distinct system for China