Table of contents

Articles

Australia
Squeezing e-commerce into old (often pre-internet) laws

Mainland China
The emergence of the new e-commerce law in a mature market

New Zealand
How do New Zealand’s new advertising standards stack up against virtual influencers?

Singapore
Upcoming regulation of payment services in Singapore

Legal updates and contacts

Australia
By Alec Christie 12

Mainland China
By Dr. Zhong Lin and Galaad Delval 16

Singapore
By Evelyn Ang and Ho Wei Yang 20

Taiwan
By Helen Fang and Fenny Kang 21

Vietnam
By Thinh Xuan Than and Jason Van Le 22

Contacts 23

Hong Kong
By Harry Lin and Philip Kwok 14

Japan
By Takahiko Itoh 15

New Zealand
By Frith Tweedie and William Fussey 17
Foreword

Welcome to our third edition of the Asia-Pacific Digital Law Newsletter, a special e-commerce edition. Firstly, all of us in EY Digital Law across the Asia-Pacific region wish you a happy, healthy and prosperous 2019 and we look forward to continuing to assist you in all your digital related endeavours this year.

This special e-commerce edition is in response to your requests after our special second edition on blockchain and cryptocurrency. Again, a request, please let us know of any topics or issues you would like us to cover in our fourth edition of the newsletter due out in July/August 2019.

In this issue we explore many of the e-commerce related developments in a number of the countries across the Asia-Pacific. Given the importance of e-commerce and the digital marketplace today, we are finally seeing a number of countries across the region introduce new laws (or amendments to existing laws) that specifically address (or catch up with) the technology and resulting processes of the digital marketplace/e-commerce. However, we are not yet seeing regional co-operation in Asia-Pacific or harmonisation of e-commerce laws to accommodate the cross-border digital marketplace or, in fact recognising the borderless nature of e-commerce.

However, if the 21st century is truly to be the century of the Asia-Pacific, the current fetters on the regional digital marketplace, imposed by each jurisdiction’s differing e-commerce laws and approaches, will need to be removed and regional harmonisation of both the approaches to and laws regulating the regional digital marketplace is required.

There is much concern in Australia about the new ‘Consumer Data Right’ and the confusion that will arise because in a few sectors (banking from July 2019 with energy and telecommunications to follow) and in specific circumstances there will be different rights and obligations applying to consumer related data. That is, different treatment of the same data in other sectors and, in the same sector, in slightly different circumstances. For the sake of certainty and consistency, let’s hope this is not a trend adopted by other countries in Asia-Pacific.

What we suspect may resonate more in other Asia-Pacific countries, late in 2018 the Australian consumer and competition regulator (the ACCC) issued its review of the digital marketplace and has recommended a focus on (and new laws/amendments to existing laws to implement) consumer’s rights (including in relation to his/her data) and significantly greater fines and enforcement (than under existing privacy law) by vesting the ACCC with regulatory oversight of all ‘consumer data’. Debate is currently raging in Australia whether (if the ACCC’s recommendations are adopted by government) this will be the death of privacy and the separate privacy regulator or a new beginning for privacy (at least in relation to us as consumers) with a regulator in the ACC with real teeth, significant fines and an enforcement track record. We suspect the themes raised by the ACCC in its review may be considered by other similar regulators in countries across the region in 2019.

Best regards, Alec

Alec Christie
EY Asia-Pacific Digital Law Leader
While Australian’s love on-line shopping (in fact all things internet), our laws have not kept pace with the ever-changing e-commerce space. Rather, in Australia, our regulators rely on businesses to interpret and adapt non-digital laws to fit the digital/on-line world. In other words, to squeeze e-commerce and digital activities into old, often pre-internet, laws.

Because of the lack of new dedicated and clearly named e-commerce or digital laws in Australia, businesses carrying on an e-commerce or digital business that is available to residents of Australia (whether that business is located within or outside Australia) often overlook the fact that all of the Australian laws strictly apply to particulars, laws relating to the carrying on of business and the interactions between customer and seller do actually apply to and in the on-line/e-commerce environment.

Although occasionally with some difficulty, the laws relating to intellectual property, contracting, sale of goods, fraud, criminal activity, gambling, censorship (and those noted below), among others, do apply and must be complied with in the e-commerce/digital environment. The four main culprits/areas of Australian regulation that are either overlooked or poorly applied in relation to e-commerce and digital transactions in/targeted at Australian residents are:

1. Consumer law
2. Privacy (including spam) law
3. E-payments regulations
4. Electronic transactions law (Federal and State)

The last of these areas are being governed by one of the few specific laws enacted to address the digital/on-line environment.

1. Consumer law

In the same way Australian consumer law applies to physical stores in Australia that sell goods to consumers, so it also applies to the on-line/e-commerce environment. The consumer law’s requirements and obligations must be complied with. In particular, the Australian consumer law imposes certain “consumer guarantees” in relation to products and services offered for sale in Australia and prohibits the exclusion of this and other consumer friendly terms in contracts and terms and conditions (T&Cs).

For those overseas companies that have e-commerce operations in Australia or are deemed to be “carrying on business” in Australia and are thus subject to the Australian consumer law, care should be taken to ensure that your local or regional standard T&Cs are reviewed, made consistent with and offer the appropriate guarantees to Australian resident consumers under the consumer law.

2. Privacy (including spam) law

Australia has robust privacy and anti-spam laws with significant penalties (up to AUD$2.1m) for breach. Whether you are an Australian or overseas) based e-commerce vendor carrying on business in Australia, you will be obliged to comply with the Australian Privacy Principles and the Privacy Act (including notifying the Privacy Commissioner and all affected individuals of any eligible data breaches).

In addition, there are very strict rules around electronic marketing (in particular by e-mail, SMS and MMS) which, effectively, mean that only those Australian residents that have expressly “opted-in” to receive commercial electronic messages (prior to receipt of such a message) may be sent commercial electronic messages. The Australian regulator responsible for this legislation, ACMA, is aggressive in its prosecution of spammers and spam, which is any commercial electronic message sent to someone who has not consented to receive such and all those who authorise, send or enable the sending of such a message.
3. E-payments regulation

Many e-commerce platforms in Australia do not establish their own e-payment mechanism, rather they outsource it to a third party provider or accept credit card payments or the like. However, even those who have outsourced the payment mechanism may still offer certain inducements or provide for gift cards, credits or the like which will require serious consideration of whether or not an appropriate Australian Financial Services Licence is required. Unlike many other countries in the region, e-payment platforms, gift cards and the like often require the provider to obtain an Australian Financial Services Licence which comes with specific conditions attached (including having an established entity in Australia).

4. Electronic transaction laws

In line with the international convention, Australia has passed a number of Electronic Transactions Acts (Federal and State) (ETAs) which permit transactions to occur via e-commerce and in an on-line context. However, the ETAs set down requirements in order for such electronic transactions to happen and default rules about when a contract will be formed, an offer accepted and the like and that a customer may opt-out of electronic transacting at any time.

We recommend that any e-commerce platform establish its own electronic transaction rules that consumers accept. This will provide certainty around many of the matters left vague in the ETAs. The ETAs also impose certain requirements around records and evidence of transactions in order to “prove” the contract between the parties involved and in respect of electronic signatures.

While electronic signatures and digital signatures can legitimately signify the acceptance of a contract and bind the relevant person or entity in Australia, care must be taken and the rules around electronic signatures should be carefully considered in order to avoid any issues in relation to the validity of contracts entered into on-line.

The good news however, as noted above, is that Australians love e-commerce and on-line shopping and any costs involved in complying with Australian legal requirements (including the above) are, we are told by clients, offset by the business that you can generate from Australian residents on-line.

Author
Alec Christie, Partner, EY Asia-Pacific Digital Law Leader, Ernst & Young (Australia)
Published on 31 July 2018 and effective since 1 January 2019, the e-commerce law was in 2018 the main law to follow in Mainland China for businesses with online activities in relation with the e-commerce ecosystem, whether if be the operation of an e-commerce platform or the operation of an e-commerce shop. Direct successor of the Administrative Measures for Online Trading (The Measures) published by the State Administration for Industry and Commerce on 26 January 2014, the e-commerce law is meant to enhance regulating the e-commerce ecosystem and to provide guidance on how the Mainland China digital economy should steer. Among the new provisions of the e-commerce law, we will in this article focus on data protection, cybersecurity, taxation and intellectual property protection that are a neat addition to the Measures.

Where is data protection?
The lack of dedicated provisions on data protection in the e-commerce law can, at first sight be unsettling. After all, Article 18 of the Measures was already providing that online e-commerce operators and their staff must strictly keep confidential and may not divulge, sell or illegally provide others with the data and information about personal information of consumers. Considering that data protection for personal information has been on the rise on a global scale during 2018, is the e-commerce law at odd, with this global trend, only relinquishing personal information protection as a general principle under its Article 5?

Data protection, far from being discarded by the e-commerce law, has in fact relegated to other laws and regulations. Article 23 of the e-commerce law states that when collecting and using user’s personal information, an e-commerce operator shall abide by the provisions regarding the protection of personal information, as stipulated in laws and administrative regulations. If this article when taken alone seems vague, we can take a glance at the previous draft of the e-commerce law, in particular its Article 20, to have a clearer idea of what type of law or regulation to look for. When done so, Article 20 refers to the Cybersecurity Law as an example of applicable laws and administrative regulations. From this it is easy to extrapolate that Article 23 refers to all and any laws and regulations that would provide for the protection of personal information, such as the Cybersecurity Law, the Consumer Law, the Advertisement Law, as well as administrative regulations with data protection provisions. From this angle it makes sense that the e-commerce law does not directly mention the Cybersecurity Law anymore, as it is meant to be paired with more laws and regulations. Solely naming the Cybersecurity Law would have led some e-commerce operators to solely focus on the Cybersecurity Law, missing out compliance with other applicable laws and regulations.

Finally, we have confirmation that the e-commerce law Article 23 is still directly intertwined with the Cybersecurity Law through Article 79, directly stating that violations of the protection of personal information in laws and administrative regulations shall be punished according to the laws and administrative regulations such as the Cyberspace Security Law of the People's Republic of China.

Relegating Cybersecurity
An intriguing article in the e-commerce law regards technical measures and other necessary measures that must be taken by e-commerce platform operators to guarantee the safety and normal operation of its network, prevent illegal crimes from being committed online, effectively respond to cyber security events and safeguard the security of e-commerce deals set in Article 30.

Article 79 of the e-commerce law states that where an e-commerce operator refuses to fulfil obligations of ensuring cybersecurity, set out in Article 30 hereof and in applicable laws and administrative regulations, it shall be punished according to laws and administrative regulations such as the Cyberspace Security Law of the People's Republic of China. While the subject of this article seems to have switched from an E-commerce platform operator to an e-commerce operator, the fact that it binds together Article 30 with the Cybersecurity Law is undeniable.
It allows us to determine that a company, whether e-commerce operator or e-commerce platform operator, to comply with Article 30 of the e-commerce law must comply with the various requirements of the Cybersecurity Law on cybersecurity. Among which is the compliance with the MLPS framework that is currently being drafted by the Ministry of Public Security.

To be kept updated on cybersecurity requirements, we strongly suggest following the development of the draft Guideline for Internet personal information security protection which is meant to impact personal information lifecycle processes in conjunction with the Cybersecurity Law, the first draft of which was released on 30 November 2018.

**Regulation and taxation**

Perhaps as expected, the e-commerce law adds provisions on the taxation of E-commerce operators that were lacking in the Measures. All E-commerce operators should now register themselves as market subjects and fulfil their tax obligations as per Article 11, although some operators can be excluded from this obligation under Article 10 if they belong to any of the following categories:

- sell self-produced agricultural and sideline products
- sell family handicrafts
- are individuals taking advantage of their own skills to engage in labor activities for the convenience of people and odd small-amount transaction activities that do not require any license under the law
- other circumstances under which no registration is required under laws and administrative regulations

Interestingly, E-commerce platform operators have a supporting role to play in the taxation of E-commerce operators. As per Article 28 they are required to actively warn E-commerce operators that have not registered themselves as market subjects about handling such registration. They need also to cooperate with the department for market regulation in providing convenience to E-commerce operators for their market subject registration.

Together, these articles form an effective double-edged obligation to greatly reduce the amount of non-registered e-commerce operators. By ensuring that each and every e-commerce operator is made aware of its obligations under law and by the e-commerce platform operator on which its business is engaged, the law ensures a greater amount of registration of e-commerce activity and thus, a higher amount of collected taxes.

**Pushing intellectual property protection forward**

The e-commerce law through Articles 41 to 45 brings intellectual property protection concerns directly under the supervision of the E-commerce platform operator. With potential fines between RMB 50,000 and RMB 500,000 or when an infraction is considered serious, between RMB 500,000 and RMB 2 million as per Article 84 for E-commerce platform operators not willing to cooperate on the protection of intellectual property.

First an e-commerce platform operator ought to set in place rules on the protection of intellectual property rights and strengthen its cooperation with intellectual property right owners as per Article 41. Such cooperation could take multiple forms, like a proactive approach to IP rights protection through the use of IP infringement seeking algorithms. However, the e-commerce law directly provides for a few cooperation channels that are mandatory and to which the E-commerce platform operator can add a supplementary layer. For example, an E-commerce platform operator is by Article 45 required to take necessary measures, such as deleting or blocking relevant information, disabling relevant links and terminating transactions and services when informed that an e-commerce operator is infringing intellectual property.

It is an interesting approach to IP protection, where the e-commerce law provides IP owners with direct remediation means through the e-commerce platform. Although implementation remains to be observed, this new cooperation and complaint channel could greatly bolster practical IP protection in Mainland China.

**What is next?**

With the e-commerce law now fully effective, what is expected next? First, we will see how e-commerce platform operators will cooperate with e-commerce operators to protect IP rights and crack-down on illegal activities. It will also be interesting to follow how e-commerce platform operators will cooperate with the State on the establishment and use of a public data sharing mechanism as described under Article 69 and how it could, in the future, synergize with the expected Social Credit Score.

**Authors**

Dr. Zhong Lin, Managing Partner, Chen & Co. Law Firm

Galaad Delval, Data Protection Officer, Chen & Co. Law Firm
“Virtual” or computer-generated social media influencers have growing appeal and influence. Can New Zealand’s advertising standards and laws keep up to maintain public confidence in advertising?

Social media influencers wield considerable power

In a world where consumers no longer trust what brands tell them, the views of trusted influencers are a seemingly authentic digital word of mouth recommendation. Social media influencers – popular online personalities with established credibility and large online followings – can endorse products and make recommendations that influence consumers’ perceptions, behaviours and ultimately purchasing decisions.

And they’re big business. Brands rely on their perceived credibility and social proof to drive sales, with some estimating the influencer market is worth in excess of $1 billion. UK research has shown that some marketers will pay as much as £75,000 for a single social media post mentioning their brand by an influencer with over one million followers. And they will pay “micro-influencers” – those with under 10,000 followers – an average of £1,500 for a mention.

The next generation of influencers

But it’s not always plain sailing for brands using influencers to promote their products. Sometimes influencers go rogue and fail to influence enough for a brand. A US PR firm is currently suing 20 year old influencer/actor/model Luka Sabbat for US$90,000 worth of “unjust enrichment” for failing to live up to his influencer obligations set out in his contract.

Breaches of influencer contracts are commonplace among both influencers and celebrities. Swipe left human influencer – hello virtual influencer.

Virtual or CGI (computer-generated image) influencers are attracting a lot of attention right now. And their numbers are expected to grow. One example is “Lil Miquela”, a 19-year old model who wears clothes from the likes of Prada and Chanel and has over a million followers.

Lil Miquela and other popular influencers like Bermuda, Blawko and Shudu are not real people. The first three are believed to be the creations of an AI and robotics start-up based in LA, with backing from several venture capital firms. Shudu is created by a fashion photographer and is known as the world’s first “digital supermodel”.

But just like their human counterparts, these virtual influencers regularly promote famous brands and products. The problem is, it’s not always clear whether their posts have been paid for by sponsors. And questions of authenticity also inevitably arise. What are we to make of posts on Lil Miquela’s Instagram account that claim beauty brands like Ouai keep her hair “silky smooth” - despite the fact that her hair is a purely digital creation? In a world that spawned Kim Kardashian and countless identikit “beauty” vloggers, what is “real” any more anyway? Is transparency still important? And who can consumers trust?

Keeping ads honest

Advertising in New Zealand is self-regulated by the Advertising Standards Authority (ASA), whose stated mission is to ensure that every ad is a responsible ad. These requirements are supported by the Fair Trading Act 1986, which prohibits misleading and deceptive conduct in trade, as well as false or misleading representations.

Recent changes by the ASA lift the bar for influencers and associated brands, requiring them to clearly identify advertisements - messages designed to influence consumer choice, opinion or behaviour where the content is
directly or indirectly controlled by the advertiser - and ensure there is “truthful presentation” of content. And giving an influencer free product in return for brand-controlled content will count as an ad just as much as making a financial payment.

The Advertising Standards Code 2018 (Code) stipulates that all advertisements must be clearly distinguishable as such, whatever their form and whatever the medium used. On Instagram, for example, Instagram users must be able to clearly understand when a celebrity post they are viewing is in fact an advertisement.

According to the ASA’s Guidance Note on Identification of Advertisements, ads may need to be identified by use of “#ad”, “Promotional Feature”, “Paid for Ad” or similar advertisement “identifiers” like logos, brand names or other visual cues. The perspective of the applicable audience will be relevant to establishing whether the advertisement is appropriately identified.

So, for example, if it’s clear from Lil Miquela’s Instagram posts that she is pushing Puma because she’s decked out head to toe in prominently branded Puma gear, and is waxing lyrical about how fabulous the brand is, then it’s possible no further disclosures will be required. This analysis will be context-specific.

“TruthfulPresentation” is a further set of ASA rules requiring that ads cannot mislead, deceive or confuse consumers, abuse their trust or exploit their lack of knowledge. Those requirements are similar to and supported by the Fair Trading Act 1986, which prohibits misleading and deceptive conduct in trade, as well as false or misleading representations.

Anything that misleads or confuses by implication, inaccuracy, ambiguity, an unrealistic claim or otherwise will breach the Truthful Presentation principle.

So Lil Miquela’s claim that a particular shampoo “keeps my strands silky smooth” when that is physically impossible could be considered an unrealistic and inaccurate claim likely to mislead, deceive or confuse consumers. If such a claim were held to be a misleading or deceptive representation, a brand could face a fine of up to $600,000 on conviction under the Fair Trading Act 1986.

What’s clear is that virtual influencers and their emerging cousins, digital humans, have arrived. For now, New Zealand’s advertising standards and laws appear able to keep up. But as artificial intelligence, social media platforms (and the huge volumes of personal information they gather), storytellers and celebrities continue to merge, it’s unclear how long that balance will last.

Author
Frith Tweedie, Senior Manager, EY Law Limited
In November 2014 Prime Minister Lee Hsien Loong revealed the vision for Singapore to be a Smart Nation. This vision entailed leveraging on technology to transform Singapore into a leading economy powered by digital innovation. To that end, key strategic national projects were identified as enablers of the Smart Nation drive – e-payments was one of them.

E-payment technologies have been significant enablers of e-commerce. However, with e-commerce poised to be the likely default mode of commerce in the future, government regulation is required as the adoption rate of e-payment services increases. In a consultation paper dated August 2016, the Monetary Authority of Singapore (MAS) proposed the idea of an activities and risk based payment framework that was “more calibrated, flexible and forward looking”. A year later, this idea was concretised when MAS issued a subsequent consultation paper on 21 November 2017, which introduced the Payment Services Bill (the Bill).

Currently, certain payment activities are regulated under the Money Changing and Remittance Business Act (MCRBA) and the Payment Systems (Oversight) Act (PS(O)A). The Bill endeavours to target more payment activities along the payment value chain with the aim of promoting “greater confidence among consumers and merchants to adopt e-payments.” The structure of the Bill comprises of two parallel frameworks. The first is the licencing regime, which aims to regulate providers of any of the seven activities that will be elaborated upon below. The second is the designation regime which has been largely imported from the PS(O)A, and has its focus on regulating payment systems whose disruption would pose financial stability risks or impact confidence in the financial system.

**Mitigating risk**
The crux of the licencing regime lies in mitigating the following areas of risk:
- money-laundering and terrorism financing
- user protection
- interoperability
- technology

Through the identification of these risks, MAS has further identified the following activities which pose sufficient risk to warrant regulation.

**First framework: seven regulated activities**
Under the licencing regime, the following are regulated activities:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic money transfer</td>
<td>Local funds transfer services in Singapore (e.g. payment gateway and payment kiosk services).</td>
</tr>
<tr>
<td>Cross border money transfer</td>
<td>Inbound or outbound remittance services in Singapore.</td>
</tr>
<tr>
<td>Merchant acquisition</td>
<td>Where the service provider contracts with a merchant to accept and process payment transactions, which results in a transfer of money to the merchant.</td>
</tr>
<tr>
<td>E-money issuance</td>
<td>Issuance of E-money in Singapore.</td>
</tr>
<tr>
<td>Virtual currency</td>
<td>Buying / Selling of virtual currency, or providing a platform for the exchange of virtual currency in Singapore.</td>
</tr>
<tr>
<td>Money-changing</td>
<td>Buying / Selling of foreign currency notes in Singapore.</td>
</tr>
</tbody>
</table>
Three classes of licences
Subject to exemptions under the Bill, service providers of any of the abovementioned seven activities (Payment Service Providers) will have to apply for a Standard Payment Institution licence or a Major Payment Institution (MPI) licence. Generally, an MPI licence is required if the Payment Service Provider oversees a large volume of transactions or provides services past the monetary threshold contemplated in the Bill.

However, Payment Service Providers who solely provide money-changing services are only required to hold a money-changing licence.

Obligations of a licensee
Under the Bill, licensees may be subjected to reporting obligations and supervision from MAS, including:

- periodic reporting
- notifying MAS upon the occurrence of specific events
- complying with notices issued by MAS
- seeking MAS approval for appointment of CEOs, directors or partners
- seeking MAS approval for persons who will become substantial shareholders

By virtue of the increased risks an MPI poses, MPIs are subject to additional obligations under the Bill, including the maintenance of security moneys with MAS and the safeguarding of customer moneys.

As the Bill has yet to be passed, the specifics and extent of regulation are currently unknown and guidance can only be taken from the MAS consultation papers and the Bill.

Carve-outs and exclusions
In line with the risk based approach, the Bill provides carve-outs for certain Payment Service Providers, such as providers of “e-money” and “virtual currency” services which are limited in user reach. It also prescribes powers for MAS to grant exemptions (including class exemptions) to Payment Service Providers from complying with the Bill.

Second framework:
Designation regime
The designation regime remains largely the same as in the PS(O)A, and MAS will continue to hold the power to designate a payment system as a designated payment system under the Bill. A new feature of the Bill, however, is the broadening of the designation criteria to include competition or efficiency reasons.

Where we are now
MAS issued the E-payment User Protection Guidelines (the Guidelines) on 28 September 2018 after taking into account the feedback received in response to its consultation paper dated 13 February 2018. These Guidelines set out MAS’ expectations of financial institutions that operate certain payment accounts, which includes the duties of account holders and financial institutions, the duties of relevant parties in relation to erroneous transactions and determining the liability of an account holder or user in the event of an unauthorised transaction.

While the Bill is likely to represent a significant change in the payments landscape, it is unclear when Payment Service Providers will be affected as the date of the implementation of the Bill is still unknown. Nevertheless, MAS has proposed a grace period of six months for newly regulated entities to submit their licence applications to MAS. Until then, Payment Service Providers would have to be kept on their toes as the Payment Services Act approaches the horizon.

Authors
Evelyn Ang, Managing Director, Atlas Asia Law Corporation
Ho Wei Yang, Associate, Atlas Asia Law Corporation
Consumer Data Rights
Legislation establishing the Consumer Data Right (CDR) is set to be introduced into Australian Parliament (and passed) early this year and is proposed to first apply to banking (i.e., open banking) from 1 July 2019. CDR data will have more onerous CDR specific privacy obligations applicable to it, instead of the generally applicable Australian Privacy Principles (APPs).

It is unclear as to how exactly the privacy safeguards of the CDR will interact with the provisions of the Privacy Act 1988. We fear that CDR will create:

- unnecessary complexity through the establishment of a second legislative regime of privacy requirements
- different classes of privacy protection depending on whether the relevant data is CDR data under the privacy safeguards or personal information under the APPs
- a situation where the same data may change from CDR data to personal information and back again and needs to be dealt with under separate privacy regimes at different times depending on its then classification
- a strict consent regime will for CDR data (irrespective of whether or not it is sensitive information)

Financial Services Cyber Standard
From 1 July 2019, the new Prudential Standard CPS 234 “Information Security” issued by the financial services regulator in Australia APRA is due to become effective. CPS 234 significantly increases the obligations imposed on APRA regulated financial services organisations (FSO) as regards information and cyber security. This includes making it clear that the Boards of APRA regulated FSO are responsible (and will be held accountable) for ensuring the information/cyber security of their organisations. CPS 234 also introduces notification to APRA of both breaches of CPS 234 and all other incidents notifiable to other regulators (e.g., notifiable data breaches under the Privacy Act).

These obligations imposed on APRA regulated FSO are in addition to the information security and other obligations under the Privacy Act/APPs.
Encryption

Criminal syndicates and terrorists use encryption to cloak messages and transactions from law enforcement and security agencies. The Australian Federal Government is attempting to bolster the investigatory capability of those agencies by introducing the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (the Act).

What do payments service providers need to know?

The Act is now law and allows federal law enforcement agencies to issue technical assistance notices (TANs) compelling a ‘designated communications provider’ to assist with enforcement efforts, which could mean:

- removing electronic protection, e.g. unlocking encrypted data
- providing authorities with physical access to IT systems
- installing, maintaining, testing or using (government-supplied) software
- providing technical information, e.g. detailed descriptions of how software works

Service providers might also receive technical capability notices (TCNs) requiring them to prepare enabling and making arrangements for future compliance with a TAN.

Whilst telecommunications and internet service providers are those most likely to be recipients of TANs and TCNs, the Act captures a very wide range of service providers, potentially including payments service providers with respect to transactions they facilitate.

What do payments service providers need to do?

Payment service providers will need to:

- Review - consider the type of data collected, handled or held about customers, what kinds of encryption or other technologies are employed to protect the data privacy and security as well as which measures could be subject to a TAN
- Prepare - staff training will be essential for compliance with the secrecy provisions and time frames. New policies, responsibilities and training modules may be necessary. A review of overall compliance operations is recommended.
On 17 September 2018, the Hong Kong Monetary Authority (HKMA) launched the Faster Payment System (FPS) alongside the existing Clearing House Automated Transfer System (CHATS). FPS is regulated by the HKMA pursuant to the Payment Systems and Stored Value Facilities Ordinance (PSSVFO), which provides statutory backing to the finality of settlement for transactions made through Hong Kong Dollar (HKD) and Renminbi (RMB) FPS by protecting the finality of settlements from insolvency laws or any other laws. FPS is a unique platform that operates on a round-the-clock basis to support instant payments in HKD and RMB with the use of mobile phone numbers, email addresses or QR codes as account proxies for the payee. FPS also enables instantaneous payments across different banks and stored-value facilities (SVFs).

On the same day the FPS was introduced, the HKMA introduced the Implementation Guideline on Common QR Code for Retail Payments in Hong Kong (QR Code Implementation Guideline). The QR Code Implementation Guideline supplements the Common QR Code Specification for Retail Payments in Hong Kong – Merchant Presented Mode (HKQR) introduced by the HKMA in December 2017, and provides recommended arrangements for merchants to combine multiple HKQR-compliant QR codes from several Payment Service Providers (PSPs) into a single combined QR code through the use of a mobile app called “Hong Kong Common QR Code”. These arrangements provide greater convenience for customers and merchants in Hong Kong - merchants will only need to show one combined QR code for receiving payments from different PSPs.
Amendments to the Personal Information Protection Act came into force last year. Under the amendments, it was made clear that data which can identify individuals such as full genome data and passport number or drivers' license number, was also to be treated as personal information. The amendment also introduced a new definition of “sensitive personal information” which includes race, creed, social status, criminal records, disability, medical, clinical and dosage records, as well as genome information. It is not always necessarily to obtain consent when collecting ordinary personal information, as well as when providing it to third parties within Japan, as long as the purpose to collect personal information is disclosed and as opt out procedure is available. However, when a personal information is recognized as a sensitive personal information it is then required to obtain specific consent for the collection of sensitive personal information, as well as its provision to third parties.

With this amendment, many medical, clinical and dosage data tied to individuals became sensitive personal information. It makes it more complex to provide such data from hospitals and other medical institution to pharmaceutical companies and other research institutes to analyze. It also makes it more difficult to use such data for improving medical and pharmaceutical practices.

In order to overcome this situation, the Diet has passed the Act concerning Anonymously Processed Medical Information to contribute to the Research and Development in the Medical Practice (Medical Big Data Act), which was implemented on 11 May 2018. Under the Medical Big Data Act, a company which satisfies certain qualifications and is approved by the government may receive sensitive personal information and process it into Anonymously Processed Medical Information so that such Anonymously Processed Medical Information can be used by pharmaceutical companies and other research institutes. It is expected that medical clinical and dosage data will be efficiently used while protecting the rights of individuals, but no company has yet applied for government approval.
On 30 November 2018, the draft Guidelines for Internet Personal Information Security Protection (The Guidelines) was published for comments by the Ministry of Public Security Network Security Bureau. These new draft guidelines are meant to guide network operators, as defined by Article 76.3 of the Cybersecurity Law, in carrying out security protection during any personal information lifecycle process.

At this stage it is unlikely that the Guidelines will be mandatory on their own. In its introduction, it is clearly stated that where specific elements of the Guidelines are otherwise stipulated by laws and regulations, they shall be implemented in accordance with such provisions. From this we can deduce that the Guidelines will be a recommendation and not a mandatory standard, unless it is required by a law or a regulation to comply with it.

Beyond the implementation status of the Guidelines, it is an important document for network operators to further understand the obligations set by the Cybersecurity Law. For example, under Article 41 of the Cybersecurity Law, network operators are required to dispose of personal information they have stored in accordance with the provisions of laws and administrative regulations and agreement reached with users. This article, while requiring deletion of personal information on the expiration of the retention period, does not provide how such deletion should occur. Using Article 6.4 of the Guidelines we are further informed that deletion should:

- Occur upon reaching the expiration of the data retention time
- Be irreversible through proper technical means

At this stage we recommend companies to familiarize themselves with the Guidelines to determine how it could impact their business in Mainland China. In particular, the Guidelines will synergize with the Personal Information Security Specifications and impact the collection and processing of personal information.
The “Algorithm Assessment Report” describes algorithms as having an “essential role” in supporting the provision of government services. While it recognises the “fresh challenges” introduced by new and evolving technology - cheerfully described as “opportunities” - the report seems keen to avoid the current media fascination with stories of killer robot armies taking our jobs and ruling the world. But does it end up downplaying the risks and does it provide a sufficiently strong base for improvement as the New Zealand government moves towards use of artificial intelligence (AI)?

First government review of its kind

The review was conducted by Stats NZ and the Department of Internal Affairs to assess existing algorithms and their uses across 14 government agencies. It’s the first review of its kind in New Zealand and internationally, with a stated objective of ensuring New Zealanders are informed and have confidence in how the government uses algorithms.

Growing public awareness of risks

Risks associated with algorithms and AI are also increasingly well known. Stories of racist robots, privacy breaches and opaque proprietary algorithms are now widely reported. Closer to home, recent high-profile headlines involving the Ministry of Social Development, ACC and Immigration New Zealand are likely to have helped focus attention on these issues.

Many of the algorithm case studies discussed in the report carry real privacy, bias and discrimination risks. For example, the Police supports decision-making by frontline staff by using two algorithms to assess the risk of future domestic violence offending. The combination is used to identify an "overall level of concern" for the safety of the people involved. But it appears that ethnicity may be a data variable in those tools, increasing risks of bias and discrimination.

Inferences like assumptions and predictions about future behaviour may also be privacy-invasive, counterintuitive and unable to be verified at the time of decision-making. The Department of Corrections uses an algorithm to calculate the probability that an individual offender will be re-convicted and re-imprisoned for new offending within five years - immediately bringing to mind the controversial COMPAS tool used in the US. While ethnicity is not a variable in the Corrections algorithm - unlike the COMPAS tool - but age, gender, age at first offence, number of court appearance and convictions all are.

Inconsistent assurance efforts

The report found an inconsistent approach to assurance around the development of algorithms, with the type and extent of such assurance varying between agencies. It makes a number of recommendations - but is light on detail of how to achieve them.
The report says government agencies should:

- develop formal policies to balance automated and human decision-making
- implement processes to ensure privacy, ethics, and human rights considerations are considered during algorithm development and procurement
- explain how algorithms may affect people in clear and simple terms
- implement processes to regularly review algorithms for unfair, biased or discriminatory outcomes
- share best practice with support from external privacy, ethics, and data experts.

What is missing?

Data quality and governance

The report found government agencies could do more to understand data limitations. It acknowledges that "without high quality data, and appropriate data management, the accuracy and predictive ability of any algorithm can be compromised".

But the report doesn't include any recommendations around what agencies should be doing to manage data quality issues – what is commonly referred to as "garbage in, garbage out" (GIGO).

As Amazon recently found out, an algorithm is only as good as the data it learns from. It scrapped its AI recruitment tool after the tool taught itself that male candidates were preferable. The problem arose because the system was trained on data submitted by applicants over a 10-year period – much of which came from men.

Comprehensive data governance strategies and processes that focus on data quality, labelling and visibility of potentially biased data will help manage GIGO and data quality risks. In addition, a set of tailored data and AI ethical principles can help organisations be clear on key privacy, data ethics and other considerations relevant to their work.

Black box risks

The report recommends greater transparency around algorithms. In an interview on Radio New Zealand, the Government Chief Data Steward advocated agencies sharing their code with the public.

But how can such transparency be achieved when confidential commercial solutions have been deployed? The report found the most common approach to the development and procurement of algorithms by agencies involved contracting external expertise into an internal development process.

Commercial partners may understandably be reluctant to share the internal workings of their algorithms for fear of disclosing trade secrets and sources of competitive advantage. But that makes it hard to monitor and challenge decisions and other outputs.

Unfortunately the report doesn't include any suggestions on how to manage these challenges. Government agencies will need to approach their procurement processes very carefully, building transparency requirements into contracts with third party providers and carefully considering issues like ownership of intellectual property. Algorithmic
Impact Assessments and monitoring for unintended consequences become even more important.

What should be done?
Overall the report is a largely comprehensive look at government agencies’ use of algorithms in New Zealand. But its perky approach risks downplaying some of the ethical, privacy and bias challenges and its recommendations lack detail.

Government decision makers would be well advised to explore the growing wealth of global insights on how to guide innovation in a way that builds and sustains trust. Leading tactics observed internationally to build algorithmic and AI ecosystems include the following.

- Ethics boards – to provide independent guidance on ethical considerations and capture perspectives that go beyond a purely technological focus. Advisors should be drawn from ethics, law, philosophy, privacy and science to provide diverse perspectives and insights on issues that may have been overlooked by the development team.

- Design standards – to help define governance and accountability mechanisms and enable management to identify what is and is not acceptable.

- Validation tools – to help ensure algorithms are performing as intended and are producing accurate, fair and unbiased outcomes.

- Internal awareness training – for executives and developers on legal and ethical considerations and responsibilities to build trust in the use of algorithms and AI.

- Independent audits – of ethical and design issues to test and validate algorithms and AI systems and evaluate governance model and controls.

The government should also consider developing a national AI strategy to pro-actively address issues such as how to harness the benefits of AI without compromising privacy, how AI should be used in specific cases and how to use AI responsibly and without bias.

China, France, Canada, Germany and, most recently, Estonia, have already taken this step. EY’s global AI Lead, Keith Strier, is a senior advisor on Estonia’s recently announced AI strategy and action plan. He says guidelines for how to deploy AI, and to what extent, will be critical for governments in the new global economy to stay relevant. “Not having a national AI action plan will mean a failure to really coordinate focused resources, which, in a smaller country is more essential because there’s more limited resources”. New Zealand would do well to follow suit.
The Payment Services Bill (The Bill) was introduced in Parliament for the first reading on 19 November 2018. Once the Bill is enacted, it will regulate payment activities along the payment value chain via two parallel frameworks.

1. Licensing Framework

The first framework is an activity-based licensing regime that will regulate service providers whose business involve the provision of any of the following seven activities (Payment Service Providers):

- Account issuance
- Domestic money transfer
- Cross border money transfer
- Merchant acquisition
- E-money issuance
- Virtual currency
- Money-changing

Subject to exemptions under the Bill, Payment Service Providers would have to apply for either a Standard Payment Institution license or a Major Payment Institution license. Generally, the latter is required if the Payment Service Provider oversees a large volume of transactions or provides services past the monetary threshold contemplated in the Bill. However, Payment Service Providers who solely provide money-changing services are only required to hold a money-changing licence.

The obligations of licensees include periodic reporting to the Monetary Authority of Singapore (MAS), complying with notices issued by MAS, and seeking MAS approval for the appointment of CEOs, directors or partners, and for persons who will become substantial shareholders.

2. Designation Framework

The second framework is a designation regime which remains largely the same as that set out in the existing Payment Systems (Oversight) Act, and MAS will continue to hold the power to designate a payment system as a designated payment system under the Bill. A new feature of the Bill, however, is the broadening of the designation criteria to include competition or efficiency reasons.

As stated in the MAS explanatory brief published on 19 November 2018, transitional arrangements of between 6 and 12 months will be provided to facilitate a smooth transition of Payment Service Providers into the new regulatory framework.
On 5 December 2018, Executive Yuan announced the following regulations to take effect on 1 January 2019:

- The new Information and Communication Security Management Act (ICSMA)
- The Enforcement Rules of Information and Communication Security Management Act,
- The Regulation of Classification of Information and Communication Security Obligations
- The Regulation of Security Breaches and Reports
- The Regulation of Audit on Non-governmental Institutions’ Information and Communication Security Plan and Execution
- The Regulation of Security on Sharing Information and Regulation of Reward and Punishment on Government Personnel for Information and Communication Security Management

The ICSMA and the relevant rules and regulations not only aim to tackle threats to government information security, but also the threats to any information security of key infrastructure providers such as hospitals or industrial science parks. As stated in Article 1 of ICSMA, the goal of ICSMA is to maintain national security and protect public interests by way of promoting the information and communication security policy, accelerating on building a safe information and communication systems.

ICSMA requires that governmental agencies and certain non-governmental institutions including key infrastructure providers, state-funded foundations, and state-run enterprises (collectively referred to as non-governmental institutes) to implement an information security maintenance plan (security plan) and establish a communication security systems (security system). The Regulation of Classification of Information and Communication Security Obligations further specifies the requirements of such plan and systems that each governmental agencies and non-governmental institution need to comply with according to its accountability, hierarchy, sensitivity and sizes of the data accessed. If any non-governmental institutions fail to comply with the security plan and security system required, a penalty ranging from NTDS$100,000 to NTDS$1,000,000 may be imposed.

Under the ICSMA, non-governmental institutions also face a higher penalty. According to Article 18 of ICSMA and Regulation of Security Breaches and Reports, where there are any events of information and security breach, non-governmental institutions are obliged to report to authorities in a timely manner, and in its breach report shall detail the investigation of the breach, coping mechanism and security improvement report. Pursuant to Article 21 of ICSMA, where any non-governmental institutions fails to report the breach events compliant with Article 18, a penalty raging from NTDS$300,000 to NTDS$5,000,000 may be imposed.
Following the Law on Cyber Security (LOCS) of 12 June 2018, companies have been waiting for the government to issue a decree on the interpretation and implementation of LOCS. On 31 October 2018 the Government issued the second draft Decree providing detailed regulations on a number of articles of LOCS.

Of particular interest is its Chapter 5 relating to the requirement for foreign providers of internet related services to open a branch or representative offices and data localization centers in Vietnam. This requirement is now restricted to companies that meet all of the following conditions:

- providing one or more of specific services to users in Vietnam, including: (i) telecommunications, (ii) internet data storage, (iii) internet data sharing, (iv) web hosting services, (v) e-commerce, (vi) online payment, (vii) payment intermediary, (viii) transportation connection service, (ix) social network and social media, (x) online gaming, and (xi) electronic mail

- carries out activities of collecting, exploiting, analyzing, and processing the data of Vietnamese users

- allowing its users to conduct activities prohibited by Articles 8.1 and 8.2 of LOCS (prohibited acts)

- breach of the provisions of Article 8.4 or Article 26.2.(a) & (b) of LOCS (providing user information and to prevent the sharing of and deletion of certain kinds of information within 24 hours of receipt of a request from the Ministry of Public Security (MPS))

Article 29 states that within twelve months from the date of a request by MPS, the company having met all of the conditions above must store data and have a branch or representative office in Vietnam.

Please note that the Decree is in draft form only and further amendments may be made.
## Contacts

### EY Asia-Pacific Digital Law services contacts

<table>
<thead>
<tr>
<th>Country</th>
<th>Contact Name</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Alec Christie</td>
<td><a href="mailto:alec.christie@au.ey.com">alec.christie@au.ey.com</a></td>
<td>+61 2 9248 4325</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Harry Lin</td>
<td><a href="mailto:harry.lin@lha.hk">harry.lin@lha.hk</a></td>
<td>+852 2629 3201</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>Takahiko Itoh</td>
<td><a href="mailto:takahiko.itoh@jp.ey.com">takahiko.itoh@jp.ey.com</a></td>
<td>+81 3 3509 1688</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mainland China</td>
<td>Dr. Zhong Lin</td>
<td><a href="mailto:zhong.lin@cn.ey.com">zhong.lin@cn.ey.com</a></td>
<td>+86 21 2228 8358</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Zealand</td>
<td>Frith Tweedie</td>
<td><a href="mailto:frith.tweedie@nz.ey.com">frith.tweedie@nz.ey.com</a></td>
<td>+64 27 836 1545</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td>Evelyn Ang</td>
<td><a href="mailto:evelyn.ang@sg.ey.com">evelyn.ang@sg.ey.com</a></td>
<td>+65 6718 1288</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Taiwan</td>
<td>Helen Fang</td>
<td><a href="mailto:helen.fang@tw.ey.com">helen.fang@tw.ey.com</a></td>
<td>+886 2 2757 1771</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vietnam</td>
<td>Thinh Xuan Than</td>
<td><a href="mailto:thinh.xuan.than@vn.ey.com">thinh.xuan.than@vn.ey.com</a></td>
<td>+84 8 3824 5252</td>
</tr>
</tbody>
</table>

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2019 EYGM Limited.
All Rights Reserved.
EYG no. 000001-19Gbl
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.