EY Asia-Pacific Digital Law Newsletter
August 2019 - Edition 4
The EY Asia-Pacific Digital Law Newsletter is a biyearly publication focusing on developments and key themes across Digital Law in the Asia-Pacific region. It includes articles as well as legal updates from all of EY Digital Law in the Asia-Pacific region.

You can consult previous issues of the EY Asia-Pacific Digital Law Newsletter on the EY Law Blog at eylaw.ey.com.

**Articles**

**Australia**
Rogue robots: Is Australia’s legal framework ready for AI stuff-ups?

**Hong Kong**
Hong Kong’s latest FinTech and AI developments in banking

**New Zealand**
Global AI Legislation - Who is doing what?

**Singapore**
Best practices in businesses’ use of AI in Singapore
Foreword

Welcome to our fourth edition of the Asia-Pacific Digital Law Newsletter, a special artificial intelligence (AI) edition.

This special AI edition is in response to your requests after our prior special editions on blockchain/cryptocurrency and e-commerce. Again, a request, please let us know of any topics or issues you would like us to cover in our fifth edition of the newsletter due out in January 2020.

In this edition, we explore the AI-related legal developments in a number of jurisdictions across the Asia-Pacific. Given both the hype around and potential of AI, we are seeing a few jurisdictions across the region introducing guidances, considering ethical frameworks and some new laws (or amendments to existing laws) that specifically address the use of AI technology. However, we are not yet seeing regional cooperation in Asia-Pacific (or globally) or a move to introduce harmonized AI laws.

Our coverage of AI developments in this edition ranges from an overview of global AI legislation from our New Zealand colleagues, through a consideration of liability for ‘rogue robots’ in Australia, Hong Kong’s latest developments in AI banking to Singapore’s recent best practices guidance on use of AI in business.

To keep you informed of what is happening around our region, we also include short updates on key developments in the Asia-Pacific in the Digital Law space.

I commend this special AI edition to you. Please do not hesitate to reach out to your relevant jurisdiction contact listed on page 25 if you wish to further discuss the material in this edition or your Digital Law needs in your jurisdiction or across the Asia-Pacific region.

Best regards, Alec

Legal updates and contacts

Australia 14 New Zealand 19
By James Wong and Alec Christie

Hong Kong 15 Singapore 20
By Kareena Teh and Philip Kwok

Japan 16 Taiwan 21
By Takahiko Itoh

Mainland China 18 Vietnam 23
By Dr. Zhong Lin and Galaad Delval

Contacts 24

Alec Christie
EY Asia-Pacific Digital Law Leader
Artificial intelligence (AI) technology has been in development for decades, yet its most powerful applications are only now becoming realities. Popular uptake of AI technology presents critical challenges for the law which, in Australia as in much of the world, remains uncertain in this emerging area.

**Can our AI technology expose the business to liability?**

Even in its relative infancy, AI has demonstrated that it can produce unexpected consequences that can cause harm/loss for which engineers, developers, owners and users of an artificially intelligent machine/robot might be liable.

The harm/loss may be physical, such as in relation to autonomous vehicles and surgical robots, as is often sensationalized in the media. Alternatively, the harm/loss may flow from AI exercising autonomous judgment where that judgment is either automatically executed or relied on for decision-making. Some examples include where:

- a robo-adviser gives advice (e.g., investment advice) which, when followed, causes loss (e.g., economic loss)
- AI technology is adopted by the healthcare sector in the hope of decreasing misdiagnoses and medical error and improving access to and affordability of healthcare. Even if this were to have a net positive effect on healthcare outcomes, who would be liable where an AI system misdiagnosed a medical condition? Unlike a human doctor, it may not be possible to justify why the AI system has come to a certain conclusion
- AI technology engages in ‘journalism’ as it did in the last US presidential election, raising questions of who would be liable if news generated turned out to be factually inaccurate (e.g. ‘fake news’), defamatory or highly sensitive/embargoed
- AI is introduced to make major infrastructure systems such as energy distribution and telecommunications systems more efficient. A bad decision made by AI, such as to prioritize one area of an electricity grid over another, could lead to significant economic loss
- a chatbot was taught how to learn from human tweets but almost immediately began publishing offensive content after hackers realized they could teach it to do so
- an AI-powered voice assistant ordered an expensive doll-house after a 6-year-old girl had a conversation with the device in her home. When a news anchor covered the story on television, quoting the child saying "[the voice assistant] ordered me a doll-house", similar devices in television viewers’ homes reportedly started ordering doll-houses too, having mistaken these words in the news report as a direction by the viewers to order a doll-house.

**This time it’s different**

In an earlier age of computing when machines thought in a linear fashion a programmer could, theoretically, list out each permutation that a computer program could arrive at. In the eyes of the law, the programmer would be able to foresee the possible outcomes of running a computer program, making it easier to foresee any harm/loss that might arise and providing relative clarity as to who is responsible. In the case of rules-based automation, the exercise of judgment can be linked to the entity that engineered or developed the automated system. A person who programmed a robotic process automation (RPA) system, for example, can be held liable for loss or harm/loss caused by that system.
In the case of AI, however, the legal position is less clear-cut. In 2019 a truly artificially intelligent system can learn on its own. It moves beyond mere automation (i.e., the rules-based, 'if this, then that’ model of computing).

For the purposes of considering how the law might treat any loss or harm/loss suffered as a result of AI technology decision-making, take the example of a self-driving car. The self-driving car takes in sensory information to learn from the world around it. Let’s say that such a car, for some reason, has made a decision to crash into a shop front injuring pedestrians, inflicting property damage and causing the shop to stop trading for a few weeks. Who is liable to compensate those who have suffered loss? When a system can learn on its own, the results that flow from that learning become difficult or impossible to predict – even for those who taught the system how to learn in the first place.

Liability might arise under:
- tort law
- criminal law
- the Australian Consumer Law (ACL)

### Liability in tort is uncertain

The legal position is, at best, murky under Australian tort law. Tort law is fundamentally connected to the notion of fault, requiring that a wrongdoer fall below some standard of behavior required by law (either intentionally or negligently). The tort of negligence in Australia asks:

- whether a duty of care exists between the wrongdoer and the harm sufferer
- whether the standard of care that should be expected of the wrongdoer was met
- and whether the wrongdoer ‘caused’ the harm suffered

In a negligence suit the first two of these three elements involve the court asking questions around foreseeability. Specifically, in finding that a duty of care exists, whether the wrongdoer ought reasonably to foresee that his/her conduct may be likely to cause loss or damage to the sufferer of harm (or a class of persons to which the harm sufferer belongs) and in determining the standard of care to which the wrongdoer’s conduct will be assessed, whether a reasonable person in the wrongdoer’s position would have foreseen that his/her conduct might pose a risk of injury to the harm sufferer (or a class of persons to whom the harm sufferer belongs). To foresee a probable consequence requires some awareness of the series of events that could lead to such a consequence. In the context of AI, where a robot learns how to think for itself, there may not be a person who could be said to have ‘foreseen’ the loss or damage that occurred. If no such person exists a person who has suffered harm because of the actions of a robot has nobody to claim damages against, leaving the question of liability uncertain.

The third element of negligence relates to causation of the harm. A court will ask whether the wrongdoer’s negligence was necessary for the harm to have occurred (i.e., ‘had there been no negligence, would the harm have happened?’) and whether it is appropriate for liability on the part of the wrongdoer to extend to the harm that was caused to the person. So causation is also about the series of events that lead to harm. Again, where a robot exercises its own ‘intelligent judgment’ it becomes difficult to identify human wrongdoers who could be said to have ‘caused’ the loss or damage. Accordingly, negligence offers little or no protection as a mechanism for allocating liability in respect of AI technology.

### Robot crime

How about criminal law? For a person to be guilty of a criminal offence, it is necessary to prove the:
- physical element
- mental element of that offence.

The physical element is some ‘act’ or ‘omission’ and, as AI technology advances, it becomes ever more difficult to ascribe a robot’s decision to a human’s act or omission. The mental element is some degree of intention or recklessness in committing the physical element. We cannot ascribe a ‘guilty mind’ to a non-human entity and robots’ decision-making processes are becoming increasingly far-removed from human intentions. At least for the foreseeable future, company directors generally need not fear criminal liability for ‘decisions’ made by AI technology.

### Robots as consumer products

Finally, AI technology may be incorporated into a product and, in addition to the law of negligence as it relates to product liability, the ACL set out in Schedule 2 of the Competition and Consumer Act 2010 (Cth) may apply. The ACL sets out protections for faulty products and includes consumer guarantees around fitness-for-purpose and quality.

### What shape is AI regulation likely to take?

Although, highly speculative, a future regulatory framework for AI in Australia might feature:
- a code of ethics
- regulatory standards
- compulsory no-fault robot insurance.
Firstly, we can expect discourse around the ethical framework on which AI legislation shall be written. As far back as 1942 science fiction author Isaac Asimov posited that, in an age of AI, widely accepted rules of ethics would be necessary and proposed his now famous ‘Three Laws of Robotics’. In some jurisdictions such as the United Kingdom, inquiries into robotics and AI considering questions of ethics have already been undertaken. In Australia the Australian Human Rights Commission together with the World Economic Forum released a white paper on AI governance in January this year.

Secondly, just as we have both legislated and industry-driven standards for goods and services today, such standards will need to be developed and agreed for AI technology. On 27 January 2017, the European Commission’s Committee on Legal Affairs passed its report suggesting a new registration system for smart autonomous robots (the EC Report). In its proposed regulatory model operation of registered robots would be subject to an advisory code of conduct to guide their design, production and use. Then, on 8 April 2019, the European Commission’s High-Level Expert Group on AI published its ethics guidelines for trustworthy AI.

Finally, it is likely that robots capable of causing harm/loss will be subject to compulsory insurance requirements. Under the EC Report’s proposed regulatory model the manufacturer, programmer, owner or user of a robot would be able to benefit from limited liability (for damage caused by a robot) if they:

- contribute to a compensation fund
- jointly take out insurance to guarantee compensation where damage is caused by the robot. In effect, this offloads both the risk and the obligation to pay damages to an insurance company (or similar entity). An insurance company is thought better positioned to take on such risk as compared to a robot owner or user.

A European Commission proposal which is very unlikely to become law in Australia is to grant rights akin to ‘personhood’ to sufficiently autonomous robots. Robots, being legal entities of their own, would then be capable of committing crimes, entering into contracts, incurring debt and could be held accountable for their own actions – much like corporate entities have legal personality. Insurance contracts would exist between the insurer and the robot directly and the risk would be allocated across those with a proprietary interest in the robot.

Conclusions
To accelerate innovation and realize the benefits of AI, Australian lawmakers must appropriately regulate AI technology sooner rather than later to provide clarity around how this liability problem will be addressed. This is likely to require bespoke AI-specific legislation.

Despite the lack of clarity in the law as it stands, any commercial AI application will, in most cases, be bought or licensed from one party to another and this will be governed by the terms of a contract. Clear contractual drafting is therefore the best means of providing clarity in relation to issues of risk and liability allocation.

Authors
James Wong, Solicitor, Digital Law, Ernst & Young (Australia)

Alec Christie, Partner, EY Asia-Pacific Digital Law Leader, Ernst & Young (Australia)
Supported by the Hong Kong Monetary Authority (HKMA), Hong Kong’s financial sector continues its move into the new era of Smart Banking. Two recent and important FinTech and artificial intelligence (AI) developments are:

- the granting of eight virtual bank licenses
- the development of AI-enabled chatbots and other tools in conventional banks.

New virtual bank licensing

According to the press releases, these eight newly licensed virtual banks intend to launch their services within six to nine months from the date of the license. It remains to be seen what technological tools these new virtual banks will adopt in using the internet and other forms of electronic channels to acquire their customers and provide banking services.

The authorization and regulation of virtual banks is governed by the Guideline on Authorization of Virtual Banks (Guideline) (last updated on 30 May 2018) issued under section 16(10) of the Banking Ordinance (BO) which allows the HKMA to prepare and publish guidelines not inconsistent with the BO for companies seeking authorization and operation of banking businesses.

Under the Guideline, a virtual bank is defined as a bank which primarily delivers retail banking services through the internet and other forms of electronic channels instead of physical branches. In other words, virtual banks will rely on the internet, rather than on physical branches, for customer acquisition and for the delivery of banking services.

Set out below are a few key points to note in applying for virtual bank licenses under the Guideline:

- Both financial firms (including existing banks) and non-financial firms (including technology companies) may apply to own and operate virtual banks.
- Virtual banks must maintain a physical office in Hong Kong, being its principal place of business, for interfacing with the HKMA and customers to deal with their inquiries or complaints. However, virtual banks are not expected to establish local branches.
- Virtual banks must meet the minimum criteria for authorization as prescribed under the Seventh Schedule of the BO (i.e., the same minimum criteria applicable to traditional banks). Among other things, virtual banks must meet the minimum paid-up capital requirement, currently HK $300 million, but are required to maintain adequate capital commensurate with the nature of their operations and banking risks undertaken.
- Virtual banks must have concrete and credible business plans for how they intend to conduct their business and how they propose to comply with the authorization criteria on an ongoing basis. Their business plan for the first three years of operation must be credible and viable, include financial projections for the operation, and strike an appropriate balance between the desire to build market share and the need to earn a reasonable return.
- Virtual banks, like conventional retail banks, are expected to play an active role in promoting financial inclusion in delivering their services, and should not impose any minimum account balance requirement or low-balance fees.
- Virtual banks must demonstrate that they will treat their customers fairly and adhere to the Treat
Customers Fairly Charter, and observe the standards in the Code of Banking Practice issued by the Hong Kong Association of Banks and the DTC Association.

Virtual banks will be subject to the same supervisory requirements applicable to conventional banks, with some requirements adapted to suit the business models of virtual banks under a risk-based and technology-neutral approach.

Virtual banks must demonstrate that they have security and technology-related controls in place which are “fit for purpose” (i.e., appropriate to the type of transactions that they intend to undertake). To this end, they must engage qualified and independent experts to perform independent assessments of the adequacy of their planned IT governance and systems and provide copies of the assessment reports to the HKMA. They must also establish procedures for regular reviews to ensure ongoing suitability having regard to developing technology.

Virtual banks must also demonstrate that they have assessed other risks that they would be subject to as virtual banks and established appropriate controls to manage the risks. At a minimum, they must have assessed the eight basic types of risks identified in the HKMA’s supervisory framework i.e., credit, interest rate, market, liquidity, operational, reputation, legal and strategic risks.

Virtual banks must provide exit plans in case their business models turn out to be unsuccessful, so as to ensure that they can unwind their business operations in an orderly manner without causing disruption to customers and the financial system.

The HKMA does not object in principle to virtual banks outsourcing their computer or business operations to third party service providers, which may or may not be part of the group owning the virtual banks. If virtual banks have material outsourcing plans, they must discuss their plans in advance with the HKMA and demonstrate that they will comply with applicable laws, regulations and guidelines, and that the outsourcing arrangements will not hinder the HKMA’s supervisory powers and duties.

AI Enabled Chatbots And Other Tools

Earlier this year conventional banks in Hong Kong launched AI enabled chatbots for answering inquiries from customers. For example, HSBC implemented a virtual assistant named “Amy”, while Hang Seng Bank launched its virtual assistants “HARO” and “DORI”, and Standard Chartered Bank introduced a virtual assistant named “Stacy”. All these chatbots are available on the respective bank’s websites and answer customer inquiries using AI technologies such as natural language processing. These chatbots are but some of the FinTech initiatives that have resulted from the collaboration between banks and technology firms as part of the FinTech sandboxes set up by Hong Kong’s regulators, the HKMA, the Securities and Futures Commission (SFC) and the Insurance Authority (IA) to expedite the development and launching of new technology products at reduced development costs.

The HKMA’s FinTech Supervisory Sandbox (FSS) which allows banks and their partnering technology firms to conduct pilot trials of their FinTech initiatives, involving a limited number of participating customers without the need to achieve full compliance with the HKMA’s supervisory requirements, was launched in September 2016. More recently, the sandboxes of the HKMA, the SFC and IA were linked up to create a single point of entry for pilot trials of cross-sector FinTech products.

As at the end of March 2019, 48 new technology products have been allowed in the FSS covering biometric authentication, soft token, chatbot, distributed ledger technologies, application programming interface, regtech (e.g. remote account opening), mobile application enhancements, notification service via social media platforms and others. More than 70 major digital banking and FinTech initiatives relating to mobile payments, biometric authentication initiatives, security tokens, and other initiatives such as chatbots powered by artificial intelligence and enhanced financial services leveraging distributed ledger technologies and social media platform integration have been launched by various banks as at September 2018.

Authors

Kareena Teh, Partner, LC Lawyers LLP
Philip Kwol, Counsel, LC Lawyers LLP
The EY Digital Law team recently conducted a global review of artificial intelligence (AI) legislation.

Overall we found only a relatively small number of jurisdictions have enacted legislation that explicitly addresses AI as at 15 February 2019, either as standalone primary legislation or provisions within existing legislation.

For those jurisdictions that have enacted AI-specific provisions in existing laws, key themes common across jurisdictions were autonomous vehicle testing and biometric data, particularly around facial recognition.

31 jurisdictions have enacted AI-specific provisions in existing legislation

For those jurisdictions yet to attempt regulation of AI, industry self-regulation and non-binding “ethics frameworks” are often used to plug any gaps. But, as an increasing number of jurisdictions publicly express an intention to enact AI-specific legislation and as an increasing number continue to develop AI strategy and governance documents, we anticipate this is likely to lead to enactment of more AI-focused legislation around the world.

Key findings
1. Only two jurisdictions have enacted standalone AI-specific legislation

Our research indicates that Taiwan and the United Arab Emirates (UAE) are the only jurisdictions to have enacted standalone primary laws specifically focussed on AI as at 15 February 2019.

Taiwan’s Executive Yuan passed the “Act for Unmanned Vehicle Technology Innovations and Experiments” on 30 November 2018. That legislation permits autonomous vehicle testing in the air, in/under the sea and on the ground, exempting autonomous vehicles – including drones - from certain traffic regulations. This law provides a regulatory sandbox that enables testing of new technologies in closed environments before deployment to the public. A Taiwanese official has stated that the law makes Taiwan “the first jurisdiction to create a regulatory sandbox to aid research and development of uncrewed vehicles”.

What’s more, the law automatically repeals provisions in other legislation that conflict with this law’s ability to grant such licenses.

We understand the idea behind this law is to enable a safe testing environment for legislation that will govern technology like AI – ad hoc regulatory sandbox if you will.

2. Numerous jurisdictions have AI-specific provisions in existing legislation

We identified 31 jurisdictions that have enacted AI-specific provisions in existing legislation, primarily in the EU but also in Brazil, Japan, Russia and Singapore. The key themes identified were:

- **Data protection laws**: In the EU, the General Data Protection Regulation includes provisions regulating the use of biometric data (for example in facial recognition) and automated decision-making, including profiling. Several non-EU jurisdictions also identified data protection legislation that could impact AI (Brazil, North Macedonia, Turkey and the Ukraine).

- **Autonomous vehicle testing laws**: Highlights for the Asia-Pacific region include amendments to Singapore’s traffic laws to create a regulatory framework for testing innovations in autonomous vehicle...
Biometric data - Russia and Sweden have both enacted laws that include specific provisions on the use of biometric data, albeit to different effect. In Russia the Federal Law on Information, Informational Technologies and the Protection of Information permits identification of citizens based on biometric personal data. In Sweden the Camera Surveillance Act supplements GDPR provisions on biometric data and protection of personal data and limits how biometric data can be used.

Japan also amended its Copyright Act in 2018 to permit the use of copyright-protected materials for machine learning purposes in certain circumstances.

3. GDPR looms large in Europe

The EU’s General Data Protection Regulation (GDPR) is likely to be relevant to the use of AI in various ways, given its focus on the personal data often required to power AI technology. Its impact cannot be ignored given the significant penalties for non-compliance, including fines of up to 20 million Euros or 4% of annual turnover - whichever is greater.

Biometric data: Under the GDPR, the definition of “biometric data” includes a reference to “facial images” (Article 4 (14)). Biometric data is considered a “special category” of data, the processing of which is prohibited unless one of a limited number of exceptions applies (Article 9). That is likely to impact AI technologies that process biometric data, including for facial recognition purposes.

Automated decision-making: Under the GDPR individuals have the right not to be subject to a decision based solely on automated processing (i.e., without any human involvement), including profiling, if it “significantly affects” them. For example, automated decisions made on online credit applications or e-recruitment (Articles 4 (4) and 22; Recital 71).

According to the United Kingdom’s (UK) Information Commissioner’s Office (ICO), this right is likely to apply to “big data” and AI tools given the ease with which AI can make decisions about people by applying algorithms and machine learning techniques to large amounts of data. The ICO notes that machine learning algorithms have the potential to make decisions that are discriminatory, erroneous, unjustified and opaque. It also recognizes that data quality is a key issue for those with information governance responsibilities in a big data context.

4. More jurisdictions are saying they will enact AI-specific legislation

As at 15 February 2019 Canada, France, Kazakhstan, Russia, Spain, Sweden, Switzerland and the USA had all publicly expressed an intention to enact AI-specific legislation in the next 12 months.

Many other Governments are also developing AI strategy or governance documents that may lead to subsequent enactment of AI legislation - for example, Singapore, China, Austria, Finland, Italy and the UK.

While the Chinese Government has not publicly expressed a formal intention to enact AI-specific legislation by February 2020, it recently amended its “Personal Information Protection Standard” which addresses automated decision-making. While not legally binding that Standard is considered highly influential as it sets out best practice expected by Chinese regulators.

Many jurisdictions are also undertaking non-legislative strategy work to boost AI development and use.

The Chinese Government has incorporated AI into the revision process for several of its National Plans, in line with its goal of becoming the world leader in AI technologies.

South Korea has similarly developed a comprehensive AI strategy, established an expert council and announced US $840 million of Government spending by 2020.

France has developed an AI strategy, created a multidisciplinary AI center, provided more than €25 million for 10 AI start-ups and is working on sectoral platforms for data sharing.

The UK set out its AI ambitions in its 2017 “Digital Strategy”, has founded a dedicated research center (the Alan Turing Centre) with a dedicated budget of £45 million for 5 years) and announced £84 million funding for further AI research.
Our observations

Existing laws and standards still apply - with more AI-specific legislation likely to come

While there may be a paucity of country-level AI-specific laws at present - which we expect to change over time - it is important to remember this does not mean AI is completely unregulated or “ungoverned”. Existing laws and legislative frameworks will continue to apply to AI. For example, the approach to liability under tort law will be relevant to the development of autonomous vehicles.

In a similar vein, the EU Parliament noted in January 2019 that “many policy aspects relevant for AI-enabled services, including rules on consumer protection and policy on ethics and liability, are covered by the existing regulatory framework on services” (see report here at pages 116 and 123). It also said that it “considers that a comprehensive law or regulation on AI should be approached with caution”.

In addition, many jurisdictions are engaged in policy and strategic work around AI which is likely to lead to more AI-specific legislation. In the EU, for example, the EU Commission’s “Co-ordinated Plan on Artificial Intelligence” provides a strategic framework for EU member states’ national AI strategies, including proposed legislation.

International obligations are relevant

International treaty obligations may also impact the types of regulatory action available to Governments. World Trade Organisation agreements such as the General Agreement on Tariffs and Trade (GATT), the Agreement on Technical Barriers to Trade and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) will play a key role in this regard. Those agreements require that regulatory measures are not more trade restrictive than necessary, subject to certain exceptions. They may also prevent regulators from enforcing standards that aren’t widely accepted around the world.

Other bilateral and multilateral investment treaties like the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) could similarly operate to restrict the scope of legislation Governments may enact. For example, the CPTPP may prohibit certain legislation that requires data localization or disclosure of source code used in AI applications.

Any AI legislation will also need to account for obligations under international human rights law, like the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights.

The United Nations Human Rights Commission has reported to the UN General Assembly the human rights implications of AI, including proposing a human rights framework for the design and use of AI technologies by states and private actors. The EU Parliament has similarly noted that “the European framework for AI must be developed with full respect for the rights enshrined in the Charter of Fundamental Rights, and in particular with respect to the principles of data protection, privacy and security”.

What will the future bring?

We expect industry self-regulation and non-binding ethical frameworks to play a significant role until formal Government regulation becomes more widespread. Many leading AI businesses, such as Microsoft, have adopted formal “ethics frameworks” to boost business and consumer trust in the use of their AI products.

Similarly, many Governments are exploring the concept of AI ethics guidelines in the absence of formal legal obligations, like the “Ethics Guidelines for Trustworthy AI” released by the EU High-Level Expert Group on AI in April 2019.

Although, the Guidelines are offered at a high level without significant details, they could form a basis for the adoption of potential new standards, practices, rules or legislation. The document is clear that the guidelines within it are to be considered the start of a process towards the development of more formal guidance, rather than a formal decision or conclusion.

This is certainly a space to watch.

Author

Frith Tweedie, Senior Manager, EY Law Limited
In recent years artificial intelligence (AI) has become an increasingly integral part of businesses’ operations and strategies, given its ability to generate actionable insights and drive efficiencies, amongst other benefits. However, concerns over algorithmic biases, the potential misuse of AI and the invasion of personal privacy have also emerged. This has resulted in a growing need for a common AI governance approach that can frame discussions around the issues and potential remedies to harness AI responsibly and ethically.

In response to such a need, the Info-communications Media Development Authority (IMDA) has worked together with the Personal Data Protection Commission (PDPC) and the Advisory Council on the Ethical Use of AI and Data, to publish a proposed Model Artificial Intelligence Governance Framework (Model Framework), the first of its kind in Asia for public consultation. Additionally, the Monetary Authority of Singapore has, together with IMDA and PDPC, developed the Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector (FEAT Principles). This article provides an overview of both the Model Framework and FEAT Principles.

**Model Framework**

The Model Framework is based on the following overarching principles:

- businesses that use AI (defined as “a set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning”) when making decisions should ensure that the decision-making process is fair, transparent, and explainable (as best as possible).

- AI solutions should center on the safeguarding of humankind’s interests, including the safety and well-being of people.

Based on these two principles the Model Framework provides guidance on how businesses can go about using AI in a responsible way:

**Internal Governance Structure and Measures**

To have sound oversight of the use of AI businesses should adapt their existing internal governance structures or implement new ones, where needed, to include appropriate features such as clear roles and responsibilities for the ethical deployment of AI, as well as a robust system of risk management and internal controls targeted at mitigating any risks resulting from the deployment of the chosen AI model.

It is also important that senior management and the board provide support, sponsorship and participation in the businesses’ AI governance.

**Determining AI Decision-Making Model**

Before implementing AI solutions businesses should weigh their commercial objectives of using AI against the risks and consider their corporate values and societal norms and values, amongst others things.

The Model Framework highlights three decision-making models with differing extent of human oversight in the process, viz, human-in-the-loop, human-out-of-the-loop, and human-over-the-loop. In ascertaining the degree of human oversight in businesses AI decision-making process they should evaluate the effects that their decisions would have on individuals using a proposed probability-severity of harm matrix.

Even after selecting the suitable AI decision-making model, businesses should regularly identify and evaluate risks relevant to their AI solutions, mitigate those risks and have an actionable response plan if mitigation does not work.
Throughout the process it is important for businesses to document every step through periodically reviewed risk impact assessments so that they are clear and confident in implementing their technology solutions.

**Operations Management**

The Model Framework sets out the following steps in the deployment of AI solutions by businesses as part of the AI adoption process:

- **Step 1:** To ensure that conclusions can be drawn accurately, raw data is formatted and cleansed. The departments within a business tasked with responsibilities over quality of data, model training and model selection should then collaborate in putting in place appropriate data accountability practices. These practices may include understanding the lineage of data, ensuring data quality, minimizing inherent bias, using different datasets for training, test, and validation, and reviewing and updating datasets from time to time.

- **Step 2:** Algorithms are applied for analysis on training datasets. The results are examined and algorithms are reiterated until a model which produces the most useful results is identified. Businesses should consider ways to increase the transparency of algorithms found in AI models through concepts of repeatability, explainability, and traceability.

- **Step 3:** The selected model is used to produce probability scores, which can be incorporated into applications to make decisions, solve problems and trigger actions. Businesses should implement internal policies and processes to conduct regular model tuning that take into account variations in customer behavior over time and to refresh models based on updated training datasets which incorporate new input data.

**Customer Relationship Management**

Businesses should engage in open communications with individuals (including employees) and adopt the following measures in implementing and managing their communication strategies when deploying AI:

- disclose whether AI is used in their goods and services
- disclose how an AI decision may impact individuals, and whether such a decision can be reversed
- conduct ethical evaluations
- develop a policy on what explanations to provide to individuals
- test user interfaces and address usability issues before deployment to ensure that the user interfaces achieve their desired object
- decide whether to give individuals the option to opt-out and whether such option should be provided upon request or by default
- put in place a feedback channel and a decision review channel for customers

**FEAT Principles**

**Fairness**

- AI or data analytics (AIDA)-driven decisions should not systematically disadvantage individuals or groups of individuals unless such decisions can be justified.

- It is justified for personal attributes to be used as input factors for AIDA-driven decisions.

**Accuracy and bias**

- Models and data used for AIDA-driven decisions should be regularly reviewed and validated for relevance and accuracy to ensure that they behave as designed and intended as well as to minimize unintentional bias.

**Ethics**

- The use of AIDA should be in line with businesses’ values, ethical standards and codes of conduct.

- AIDA-driven decisions should at least meet the same ethical standards as human-driven decisions.

**Accountability**

- The use of AIDA in AIDA-driven decision-making should be approved by a suitable internal authority.

- Businesses that use AIDA should be held accountable for both externally sourced and internally developed AIDA models.

- Businesses that use AIDA should, on their own initiative, raise management and board awareness of their use of AIDA.

- There should be channels through which data subjects can inquire about, submit appeals for and request reviews of AIDA-driven decisions that impact them.

- When conducting a review of AIDA-driven decisions, verified and relevant supplementary data given by data subjects should be considered.

**Transparency**

- Businesses should, on their own initiative, disclose to data subjects their use of AIDA as part of general communication.

- Businesses should provide data subjects, upon the latter’s request, with clear explanations on what data is used to make AIDA-driven decisions about the data subject, how the data impacts the decision and the effects that AIDA-driven decisions may have on the data subjects.

To conclude, while both the Model Framework and FEAT Principles are not legally binding they nevertheless provide much needed clarity and guidance on the good practices that businesses should adopt in their deployment of AI solutions in their operations.

**Authors**

Evelyn Ang, Managing Director, Atlas Asia Law Corporation

Victor Looi, Associate, Atlas Asia Law Corporation
A major change to employee privacy in Australia

In Australia there is an exemption from the Privacy Act 1988 (Cth) and the Australian Privacy Principles (collectively APPs) for "an act done, or practice engaged in, by an organization that is or was an employer of an individual in respect of acts or practices directly related to a current or former employment relationship between the employer and the individual and the employee record held by the organization and relating to that individual". An "employee record" is defined to include, among other things, the terms and conditions of employment, an employee’s personal emergency contact details, performance or conduct information, salary or wage information, membership of any professional trade association(s), long service and sick leave balances, the employee's taxation, banking or superannuation affairs and the like.

To date this exemption has been interpreted as a complete exemption from all the obligations under the APPs for the employer in respect of all employee records. That is, until now, none of the APPs relating to the collection, use or disclosure of personal information were considered to apply to the employer of the relevant individual in respect of his/her employee records.

However, in a recent decision of the Full Bench of the Fair Work Commission in Jeremy Lee v Superior Wood Pty Ltd [2019] this interpretation has been “turned on its head”. The Full Bench, interpreting the words literally as they appear in the APPs, decided that the employee records exemption does not apply (i.e., the employer is not exempt from the provisions of the APPs in relation) to the collection of any personal information from an employee which ultimately forms part of an employee record.

That is, while it applies once held, it does not apply to the original collection of personal information.

Thus, employers are required to have a privacy policy/ statement for employees, notify that policy/statement prior to or at the time of collecting general personal information and obtain consent for collecting sensitive information from employees.

In the circumstances of this case, it meant that Mr Lee was entitled to withhold his consent to the collection of his sensitive (i.e., biometric) information and thus legitimately not use his thumbprint to clock on and clock off from his place of work.

This decision has significant ramifications for all employers in Australia, especially those collecting sensitive information (e.g., thumbprint security measures, drug and alcohol testing and the like). It means that most employers in Australia will need to review their employee privacy processes (collection of information), provide an appropriate employee privacy policy (which should likely be separate to the public-facing privacy policy) and obtain consent to collect any sensitive information and the best time to do that will be at the time of joining the company (e.g., in their contract of employment).

Although, the Full Bench cautioned that consent where an employee is told (or it is implied) that he/she either consents or lose their job, is not actually consent under the APPs. This will particularly impact in the introduction of new measures requiring sensitive information after staff are already employed.
On 28 March 2019 the Hong Kong Securities and Futures Commission published a statement reiterating that security tokens (i.e., digital representations of ownership of assets (e.g., gold or real estate) or economic rights (e.g., share of profits or revenue) utilizing blockchain technology, are likely regarded as “securities” under the Securities and Futures Ordinance (SFO).

As such, they are subject to Hong Kong’s securities laws. Thus, unless an applicable exemption applies, any person who markets and distributes security tokens (whether in Hong Kong or targeting Hong Kong investors) is required to be licensed or registered for Type 1 regulated activity (dealing in securities) under the SFO.

It is a criminal offence for any person to engage in regulated activities without a license unless an exemption applies.

Intermediaries who market and distribute security tokens should ensure compliance with all existing legal and regulatory requirements, including relevant paragraphs under the Code of Conduct, as well as the selling restrictions, due diligence and information for clients requirements under the Circular to Intermediaries on Distribution of Virtual Asset Funds.
On 27 May 2019 the notification regarding the Foreign Exchange and Foreign Trade Act (the Foreign Exchange Act) was amended and 20 IT/Communication related industries were added as industries that require prior notification for Inbound Direct Investment and Specific Acquisition (both defined below). This notification will be implemented from 1 August 2019.

This amendment strengthens restrictions on entry of foreign-affiliated companies into the IT/Communication field in Japan. Foreign investors who intend to invest in Japan will need to assess whether they require prior notification in broader scope and, if so, how long it will take to obtain clearance.

1. Inbound Direct Investment and Specific Acquisition

Inbound Direct Investment is defined as the acquisition of unlisted shares (Article 26, Paragraph 2, Item 1 of the Foreign Exchange Act) and the acquisition of 10% or more of listed shares (Item 3 of the same Paragraph). Specific Acquisition is defined as acquiring unlisted shares from other foreign investors (Paragraph 3 of the same Article).

Most of these activities only require post transaction notification, but when foreign investors make Inbound Direct Investment, or Specific Acquisition in Japanese companies which are doing businesses in specific industries designated by the government they need to make prior notification to the Finance Minister and other competent minister (Article 27, Paragraph 1 and Article 28, Paragraph 1 of the Foreign Exchange Act).

This regulation is intended to prevent the outflow of technology and products leading to military diversion and the occurrence of situations that have a significant impact on Japanese security, triggered by investment by foreign investors.

In principle, if the obligation for prior notification is triggered, activities which fail under Inbound Direct Investment and Specific Acquisition will be prohibited for the 30-day examination period after the notification. If the Ministers deem it necessary the examination period may be extended up to 4 months (Article 27, Paragraph 2, Item 3 and Article 28, Paragraph 2, Item 3 of the Foreign Exchange Act).

In 2008, when a UK investment fund tried to increase its share holding in a Japanese electric power company, the Minister ordered it to cease the transaction due to concern regarding the effect on stable supply of electricity.

The Finance Minister and the competent Minister may also order foreign investors who have acquired those shares without notification to dispose of the shares and take other necessary measures (Article 29 of the Foreign Exchange Act). In addition, if you acquire shares without notification or by ignoring cessation order, you will be subject to a fine of up to three times the amount acquired or one million yen whichever is higher (Article 70, Items 22 and 26 of the Foreign Exchange Act).
2. Addition and expansion of target industries

The 15 newly regulated industries are as follows.

(1) 10 types of information processing related equipment/parts manufacturing industry

- a. Integrated circuit manufacturing industry
- b. Semiconductor memory media manufacturing industry
- c. Optical disk, magnetic disk, magnetic tape manufacturing industry
- d. Electronic circuit board manufacturing industry
- e. Wired communication equipment manufacturing industry
- f. Mobile phone / PHS phone manufacturing industry
- g. Wireless communication equipment manufacturing industry
- h. Computer manufacturing industry
- i. Personal computer manufacturing industry
- j. External storage device manufacturing industry

(2) Three types of information processing software manufacturing industry

- a. Contract development software industry
- b. Embedded software industry
- c. Package software industry

(3) Information and communication service related industry

2 types

- a. Wire broadcasting business
- b. Information processing services

The five industries, regulatory scope of which have been expanded, are the following information communication service related industries. Previously, prior notification was required only for those businesses which required registration as telecommunications businesses under the telecommunications business law, but such limitation was removed.

- a. Local telecommunications industry
- b. Long distance telecommunications
- c. Other fixed telecommunications
- d. Mobile telecommunications
- e. Internet use support business

Until now restrictions on inbound investments focused mainly on industries related to weapons and aircraft industries but, as a result of the amendment to Foreign Exchange Act notification, industries related to AI and robots, mobile phones, personal computers, semiconductor memories which were not covered under the current framework became subject to prior notification.

It is said that those industries are referring to the 14 Emerging Technologies areas which were picked up by the United States government as new export restrictions in November 2018.

3. Intention for the amendment

The intention behind the amendment is said to be to properly prevent the occurrence of significant incident that may have significant impact on Japanese national security including, but not limited to, leakage of critical technologies and the loss of Japan's defense production and technology basis, while the importance of cybersecurity is increasing. It is also said that there is a purpose to correct the situation that Japan may become a loophole while US and European jurisdictions have tightened restrictions on inbound investment to prevent IT technology outflow and to strengthen cybersecurity policy against China and other jurisdictions subject to economic sanctions.

The US enacted the United States Defense Power Act 2019 in August 2018 and, among others, 14 areas were illustrated as a subject of export restrictions under the US Export Administration Reform Act (ECRA), with China in mind. In May 2019 the US government declared a policy to embargo China's major telecommunications equipment manufacturers.

The investment screening is being strengthened in Europe as well. For example, in January 2019 France added semiconductors, robotics, cybersecurity, data centers to the industries subject to screening.

However, the areas for which regulations have been tightened under the Japanese Foreign Exchange Law Notification at this time include areas in which Japanese companies already have contracted or withdrew their businesses and we need to carefully monitor what kind of effect of influence this regulation will have.
On 13 June 2019 the Cyberspace Administration of China (CAC), the public authority overseeing cybersecurity in mainland China as per Article 9 of the Cybersecurity Law, issued the Draft Administrative Measures on Evaluating the Security of Transmitting Personal Information Overseas (个人信息出境安全评估办法(征求意见稿) the 2019 Draft Measures). The 2019 Draft immediately reignited worries of data localization being generalized in mainland China as in 2017 when the CAC issued the Draft Administrative Measures on Evaluating the Security of Transmitting Personal Information and Important Data Overseas (个人信息和重要数据出境安全评估办法(征求意见稿) the 2017 Draft Measures).

Comparing the 2019 Draft Measures with the 2017 Draft Measures, we can ascertain that the 2019 Draft Measures does not create a data localization regime supported by exclusion clauses. While Article 2 of the 2017 Draft Measures stated that “Network Operators shall store personal information and important data gathered and produced during operations within the territory of the People’s Republic of China”, Article 2 of the 2019 Draft Measures states that “Where a network operator intends to provide the personal information it has collected during its business operations within the territory of the People’s Republic of China overseas, a security assessment shall be conducted in accordance with the Measures”.

Currently, personal information is allowed for transfer overseas subject to some exclusions. Such exclusions apply to certain sectors such as the data localization of personal financial information for the Finance and Banking industry, or the status of the operator, like the data localization obligation for personal information and important data set by Article 37 of the Cybersecurity Law for Critical Information Infrastructure operators.

However, if the 2019 Draft Measures is enacted it will significantly change the current framework for cross-border transfer of personal information overseas. The framework will shift toward being approval-based in accordance with Article 4 and 5 of the 2019 Draft Measures, which requires network operators to first declare certain information to the provincial-level cyberspace department for review.

Although, the 2019 Draft Measures does not require general data localization for network operators in mainland China, we can expect companies to react defensively to the approval framework. Such reaction could take the form of using data localization by default to subtract themselves to the need to perform such assessment and to remain under the radar for the authorities. If confirmed, this would greatly disrupt numerous companies’ internal and external data processing involving overseas transfer of personal information.

It is likely that the mutation of the personal information framework of few excluded industries and operators to an approval-based system will not be positively received by companies with important or critical cross-border transfer of personal information processing. We can expect a similar response as was given to the 2017 Draft Measures and potentially a softened second draft that could ease the means of transfer, such as by modifying the approval process to a self-review process.
Copyright law reform - New Zealand

New Zealand is conducting a comprehensive review of its copyright regime to ensure it keeps pace with digital developments. The last significant review of the Copyright Act 1994 took place over a decade ago and, since then, new technologies and data uses have fundamentally changed the way New Zealanders create, distribute and consume creative works.

Liability of online platforms, exceptions for ISPs, treatment of user-generated content and protection of Māori creative works are among the issues under consideration in the Issues Paper released last November. Other key issues include:

• **Who owns the AI-generated output?** Unlike the copyright laws of many jurisdictions, New Zealand’s copyright law expressly recognizes that copyright works may be “computer-generated”. But despite this forward-looking approach, it’s not clear who in practice will own the copyright in an AI-generated work given the range of people that may be involved in the AI’s development and use.

• **Database ownership.** New Zealand law does not have specific enforceable IP rights in data or databases so this is another area where change would be welcome.

It is hoped the copyright law review will provide greater legal certainty to encourage the ongoing development of the technology and creative industries in New Zealand.

Privacy law reform update - New Zealand

A recent report on New Zealand’s Privacy Bill by the Justice Select Committee recommends some sensible changes and clarifications to the draft bill. But critics are concerned it doesn’t go far enough to keep up with global privacy law reform.

The Select Committee has recommended a higher threshold for notification of privacy breaches (from “harm” to “serious harm” in line with the Australian approach), legislative clarification that New Zealand privacy law will apply to foreign entities “carrying on business” in New Zealand and clearer rules use on the use of third parties like cloud service providers.

However, while the Privacy Bill aims to better align New Zealand with international privacy law developments, it misses many of the key components of EU’s General Data Protection Regulation, for example, which could put the jurisdiction at risk of losing its coveted EU adequacy status. Concern also persists as to the lack of real and meaningful consequences for non-compliance - the maximum fine on conviction for an offence under the Bill is NZ $10,000, in stark contrast to the potential for substantial fines under the GDPR and the proposed significant increase in fines under Australian privacy law.
As part of the Singapore Government’s drive to embrace automation-related technology, the Ministry of Transport recently made the Road Traffic (Autonomous Motor Vehicles) Rules 2017 (the Rules) pursuant to the Road Traffic Act (Cap. 276) of Singapore, to govern the trial and use of autonomous motor vehicles (AMVs) in Singapore.

Under the Rules, a person must not undertake any trial of automated vehicle technology or an AMV on any road, or use on a road an AMV, unless the person has applied for and obtained authorisation from the Land Transport Authority (LTA).

Upon receiving authorisation the person must, before the approved trial or approved special use starts, have in place liability insurance issued by an insurer who at the time of issuance is lawfully carrying on an insurance business in Singapore and ensure that such insurance is in force throughout the duration stated in the authorisation. However, if the person has made reasonable efforts to obtain such insurance but is unable to do so, LTA may allow the person to deposit with LTA a security deposit of not less than S$ 1.5 million.

In addition to fulfilling any conditions imposed by LTA in granting authorisation, the person has to ensure the maintenance of AMVs used, operation of data recorders in AMVs, keeping of records and notification to LTA of incidents and accidents in relation to the approved trial or approved special use and cooperate with LTA should LTA require the AMVs or any related items to undergo tests.
Financial technology (i.e., FinTech) has been rapidly transforming numerous aspects of the economy and financial services nowadays, as well as subverting conventional business models by enabling and facilitating the entry of non-financial firms into markets where regulated financial institutions had always been the main intermediaries for transaction flows. Elevations of artificial intelligence regarding information technology such as big data analytics also provide the assistance of financial institutions to efficiently customize the products and services to tailor-make the needs of their clients and gain a better understanding of the risk preferences of potential customers.

To regulate the trend of the financial innovation era, allow financial institutions or non-financial firms to design usable policies and prevent certain financial related regulations or moral-hazard problems, the Legislative Yuan in Taiwan passed a bill called “Financial Technology Development and Innovative Experimentation Act” (as FTDIEA, hereinafter as the Regulatory Sandbox) on December 29, 2017, and took effect on April 30, 2018. Taiwan is the first jurisdiction of the civil law system among the world to pass the Regulatory Sandbox. The aim of the legislation is to construct a secured environment for FinTech experimentation involving innovative financial technologies and develop technology-based innovative financial products or services, facilitate the development of inclusive financial systems and financial technologies, and put into effect the protection of innovative experimentation participants and financial consumers.

The competent authority responsible for the administration of the Regulatory Sandbox in Taiwan is the Financial Supervisory Commission (FSC). The period of innovation experiment is limited to 1 year and can be extended one time for a maximum of 6 months.

If the experiment involves the law for further amendment, then the times of extension for such project will not be limited but the whole term shall not exceed 3 years. An individual, sole proprietorship, partnership or legal person may apply to the competent authority for approval to undertake innovative experimentation. Therefore, innovation experiments carried out in the Regulatory Sandbox contain business opportunities for technological development in the future for applicants of either financial institutions or non-financial firms.

With the measurement of the nature and the result of the innovation experiments as well as the licensing in advance, the applicants can achieve their suitable policies and promote further value of innovation as early as possible. However, the participants are exposed to high level of risks since the Regulatory Sandbox is designed to transcend current laws and regulations. Accordingly, the FTDIEA presents certain protective measures such as stipulating the applicant’s liabilities to the participants and regulating the applicants to provide participants suitable protective and compensation measures from the innovation experiment as the obligation and related risks must be clearly defined in the contract. If the innovative experimentation involves any situation that:

- is materially adverse to the financial market or the interests of participants
- outsteps the scope approved by the FSC
- violates the additional requirements and obligations set by the FSC if the applicant fails to comply with the regulation and fails to take remedial action within the given time period as ordered by the FSC
Then the FSC may revoke the approval for the innovative experimentation and disclose the date of the revocation and reasons on its website.

One year after the implementation of the Regulatory Sandbox in Taiwan, the FSC announced their application target for the first year had been achieved. FSC had approved three applications for the experimentation and 7 more applications have been filed. The first approved case is the cooperation between KGI Securities Co. Ltd. (KGI) and Chunghwa Telecom Co., Ltd., which was approved in September 2018 and started experimenting in December. The case involves using mobile phone numbers to identify the users’ authentication and confirms their financial situation as well as the credibility through the payment of telecom bills and subsequently approves the applications of the customers regarding credit cards and micro-finance online. According to the first report of KGI, over 2,000 customers downloaded the experimental application in 3 months and they had certified over 2,000 identities. Further, there were over 100 loans signed with the allocation up to NT$ 20 million. The average loan per case was NT$ 100,000 to 200,000. No bad debts overdue 30 days were reported, nor were there any consumer disputes and fraud. The FSC stated that the experimental results will indeed help the improvement and the efficiency of the financial innovation models and is planning to open the on-line application of banking business for consumers.

The other two approved cases were with respect to small cross-border remittances for foreign migrant workers, which were approved in January this year and entered the experiment in April. The results are still under observation. As for the other 7 applications for sandboxing which are under review, there are two banks and two non-financial institutions, including CherryPay, an international peer-to-peer money transfer matching platform, which is applying for experimental banking business for cross-border remittances. Certain banks are applying to experiment with the blockchain technology for mobile phone cross-bank payments. A securities and futures industry company and a non-financial industry company are applying for a securities and futures business experiment, while another insurance company is applying for a cross-industry cooperation by selling travel insurance on an e-commerce platform. For the time being, the effectiveness of implementation of Regulatory Sandbox remains a topic for further observation.
Following the Law on Cybersecurity (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. However, as of June 2019, there is still no statement from the government regarding the additional amendment the draft or issuance an official decree guiding on the LOCS.

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

- providing one or more of specific services to user 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))

In respect of data archive, the draft Decree stipulates three following types of data to be mandatory stored in Vietnam and applied the necessary protection measures to ensure data security requirements:

I. Personal information of service users in Vietnam, including: full name, date of birth, place of birth, nationality, occupation, title, place of residence, contact address, address email, phone number, identity card number, personal identification number, citizen identification number, passport number, social insurance card number, credit card number, health status, records medical, biometrics.

II. Data created by service users in Vietnam, including information on uploading, synchronizing or importing from the device.

III. Data on the relationship of service users in Vietnam, including: friends, groups where users connect or interact.

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.

Most importantly, the lack of legal documents on sanctions and penalties towards violating regulations on data archive does not exclude enterprise from any responsibilities and risks if breaching as the draft Decree stipulates that enterprises that do not comply with the regulations on data storage, setting up branches or representative offices at Vietnam shall, depending on the nature and seriousness of the violation, be handled according to law provisions.
Contacts

EY Asia-Pacific Digital Law services contacts

**Australia**
Alec Christie
alec.christie@au.ey.com
+61 2 9248 4325

**Hong Kong**
Kareena Teh
kareena.teh@eylaw.com.hk
+852 2629 3207

**Japan**
Takahiko Itoh
takahiko.itoh@jp.ey.com
+81 3 3509 1688

**Mainland China**
Dr. Zhong Lin
zlin@chenandco.com
+86 21 2228 8358

**New Zealand**
Frith Tweedie
frith.tweedie@nz.ey.com
+64 27 836 1545

**Singapore**
Evelyn Ang
evelyn.ang@sg.ey.com
+65 6718 1288

**Taiwan**
Helen Fang
helen.fang@tw.ey.com
+886 2 2757 1771

**Vietnam**
Michael Beckman
michael.beckman@vn.ey.com
+84 28 3824 5252

For further inquiries on Digital Law services, please visit our website

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

© 2019 EYGM Limited.
All Rights Reserved.

EYG no. 003608-19Gbl

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.