Asia IP

Informed Analysis

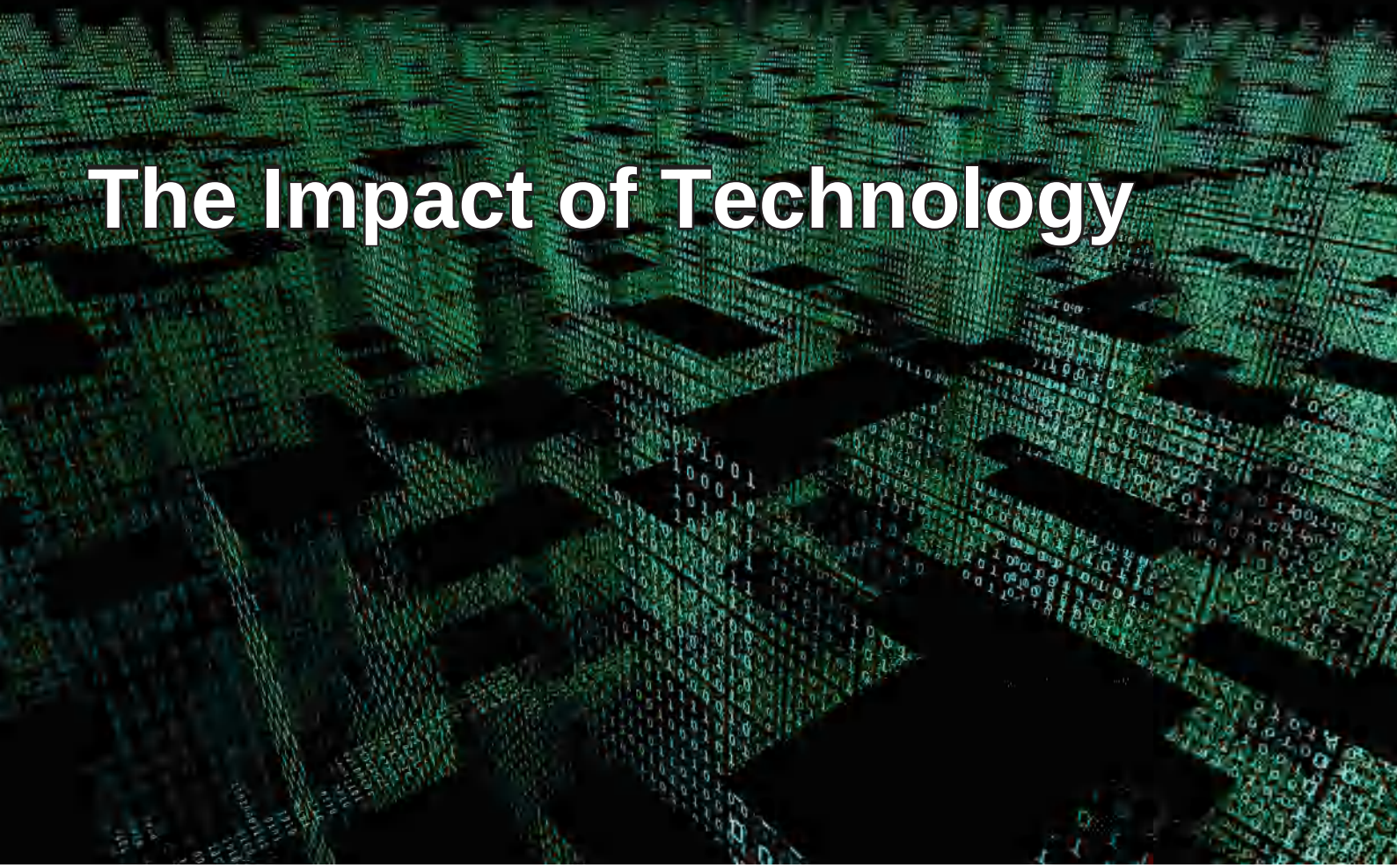
October 2016

Vol. 8 Issue 9

LANDMARKS

The Standout Cases in Asia

Apex Asia



The Impact of Technology

Johnny Chan speaks to lawyers across jurisdictions about their privacy laws, outsourcing trends and the future of boutique firms.

The Indonesian Ministry of Communication and Informatics states that there are around 82 million internet users domestically, which puts Indonesia eighth globally in terms of numbers of internet users. Eighty percent of the domestic internet users are between the age of 15 and 19. As for Facebook users, Indonesia is ranked fourth for having the most users worldwide. “This is a tremendous achievement in the field of informatics,” says Toeti Heraty N. Roosseno, president director at Biro Oktroi Roosseno in Jakarta. “However, behind these increasing numbers, Indonesia should also be aware of the risks since using the internet may sometimes expose personal data to the wrong hands.”

According to the data obtained by the Indonesian government in 2015, there are increasing threats to security information, namely malware, 996 cases; phishing, 52 cases; spam, 67 cases; and brute force attacks, 13 cases. “The actual numbers may be greater than the above statistics,” Roosseno says. “This shows that the growth of IT has caused a negative impact, and to reduce that, our government has formulated regulations to stipulate stricter [enforcement of laws].”

The ministry is also discussing a new ministry regulation concerning data protection for electronic systems. The provisions, which have been set out in a draft regulation, shall combine the self-regulation model, which has been implemented in the US, as well as in many European countries, and is commonly referred to as safe harbour principles, says Roosseno.

The draft of the regulation will regulate data collection and acquisition, with an approval, confidentiality option, and right of data revision along with verification to the data owner, Roosseno says. “Therefore, in the future, displaying, publishing, transmitting and disseminating private data will only be allowed upon the approval of the data owner, unless otherwise regulated by the laws.”

High-profile cyber attacks do not occur in great numbers in Indonesia, she says. “The cases here mostly target individuals, and there are no reports of big companies experiencing high-profile cyber attacks. Furthermore, handling cases related to cyber crimes would be quite difficult in terms of providing evidence.”

Effective November 15, 2013, the Malaysian Personal Data Protection Act 2010 provides for the protection of sensitive and personal data in commercial transactions. The act ensures that there is adequate protection for data subjects, especially in relation to classes of data users that must register with the Department of Personal Data Protection. These classes, pursuant to the Personal Data Protection (Class of Data Users) Order 2013, will include the communications sector, where a licensee under the Communications and Multimedia Act 1998 will have to be registered as a data user and comply with the requirements of the Act, says Timothy Siaw, a partner at Shearn

Delamore & Co in Kuala Lumpur.

The act practices seven personal data protection principles as follows:

General Principle. Sets out the rights and obligations of the data users whilst processing personal data.

> A special cyber court has been established in Malaysia to hear an increasing number of cyber criminal cases involving bank fraud, hacking, cyber attacks, web defacement, **document falsification, defamation,** spying, online gambling and pornography.
>
> *- Timothy Siaw, partner,*
>
> *Shearn Delamore & Co, Kuala Lumpur*

Notice and Choice Principle. Written notice must be given to data subjects so that they will know their personal data are being processed by or on behalf of the data user, the purposes for which the data is collected and processed, individual right to request correction or access to personal data, limitations imposed on the processing of the data and whether it is obligatory or voluntary for the individual to supply the data and the consequences of failure to do so.

Disclosure Principle. It must be with the consent of the data subject that personal data can be disclosed, unless it is for the purpose it was originally collected.

Security Principle. Practical steps have to be taken by the data user to safeguard the personal data from any loss, misuse, modification, unauthorized or accidental disclosure, alteration or destruction. Pursuant to the recent Personal Data Protection Standard 2015, the practical security steps includes the following:

1) Safeguarding the computer systems from malware threats to prevent attacks on personal data;

2) Registration of all employees involved in the processing of personal data;

3) Establishing physical security procedures to control the movement in and out of the data storage site, to store personal data in an appropriate location which is unexposed and safe from physical or natural threats and if necessary, provide a closed-circuit camera at the data storage site and 24 hour security monitoring.

Retention Principle. The data processed should not be retained or kept longer than necessary for the fulfillment of the purpose.

Data Integrity Principle. Reasonable steps have to be taken to ensure that the personal data is accurate, complete, not misleading and kept up-to-date.

Access Principle. Any data subject has to be given access to the personal data held by the data user and must be able to correct it.

"The act restricts the cross-border transfer of personal data under Section 129 unless it is to a place specified by the minister, taking into consideration that the place has enforced any law similar to the act or has a similar level of protection," Siaw says. "Cross-border transfer of personal data is allowed where, amongst other things, the data subject has given his consent to the transfer or it is necessary for the performance of a contract between the data subject and user. A written notice must be given to data subjects where there is a transfer of the personal data to third parties, including any person who is not the data user."

The act creates a number of criminal offences. The most relevant are:

- **Section 5,** which makes it an offence to contravene the personal data protection principles. Upon conviction, the data user will be liable to a fine not exceeding RM300,000 (US$73,000) and/or to imprisonment for a term not exceeding two years;
- **Section 16,** which prohibits processing of data by person who belong to the class of data users specified without a certificate of registration issued; and
- **Section 38,** where it is an offence to process personal data

> The most effective measures for preventing cyber attacks and addressing personal data intrusion issues would be the measures requiring data users to safeguard the computer systems from malware threats.
>
> *- Kah Yee Chong, associate,*
>
> *Tay & Partners, Kuala Lumpur*

after the data subject by notice in writing withdraws his consent to the processing. There is a fine not exceeding RM100 (US$24) and/or to imprisonment for a term not exceeding one year.

In terms of containing cyber crimes, the main legislation in relation to such enforcement and misuse of computers in Malaysia is the Computer Crimes Act 1997. This act sets out the following as criminal offences:

1) Unauthorized access to computer materials including hacking (Section 3 of the act), under which the defendant will be liable to a fine not exceeding RM50,000 (US$12,000) and/or imprisonment not exceeding five years;

2) Unauthorized access with intent to commit or facilitate commission of further offence (Section 3 of the act);

3) Unauthorized modification of the contents of any computers (Section 5 of the act); and

4) Wrongful communication of a number, code, password or other means of access to a computer to any person other than the person to whom he is duly authorized to communicate (Section 6 of the act).

Cyber Security Malaysia (the national cyber security specialist agency under the Ministry of Science, Technology and Innovation) is the regulator tasked with the enforcement and publication of cyber security related rules and guidelines. It provides for various services including the following:

1) MyCert, the Malaysia Computer Emergency Response Team providing emergency response on computer security related matters such as cyber harassment, malware, intrusion, hack attempts and other information security breaches;

2) The Digital Forensics Department (CyberCSI) to provide for, inter alia, data, audio, video, and mobile phone forensics; and

3) Certification service against the internationally recognized standard ISO/IEC 27001 accredited by Standards Malaysia.

"A special cyber court has been established in Malaysia to hear an increasing number of cyber criminal cases involving bank fraud, hacking, cyber attacks, web defacement, document falsification, defamation, spying, online gambling and pornography," Siaw says. "The court will be technologically-equipped to function as an e-court, with the necessary tools to ensure that the proceedings will go on without delay. Twenty-seven judges have undergone training programmes to enhance their knowledge on cyber-related laws."

> "Privacy by design' has become the watchword for organizations where **significant value is derived from the** collection, use and potential sharing of personal data.
>
> *- John Hannan, partner,*
>
> *DLA Piper New Zealand, Auckland*

In an effort to reduce the risk of cyber attacks and avoid data breaches, the commissioner has recently issued the Personal Data Protection Standards 2015, which came into force on December 23, 2015. The standards are intended as guidelines to be observed by the data users and implemented as part of the data users' policy in the course of processing of personal data whether through electronically or conventional means, in which case the standards required would be different, says Lin Li Lee, a partner at Tay & Partners in Kuala Lumpur.

Security measures for electronic records under the standards include restricted access, controlling transfer of personal data through removable media device and cloud computing device, password protection and security monitoring. "Amongst all, the most effective measures for preventing cyber attacks and addressing personal data intrusion issues would be the measures requiring data users to implement and update the back-up or recovery system and anti-virus as well as to safeguard the computer systems from malware threats," says Kah Yee Chong, an associate at Tay & Partners in Kuala Lumpur. "In addition, data processors are also required to comply with specific security requirements imposed by data users."

Following the concomitant increase in public awareness of data protection and regulatory changes, there is an increase in data users seeking advice and assistance on compliance with data protection laws where the business transactions often involve complex cross-border data protection issues, Lee says. "This has no doubt brought about an uptrend in work for law practices."

> "Among other obligations of data controllers and processors is a requirement to develop the personal data processing system and register this with the National Privacy Commission.
>
> *- Rose Marie M. King-Dominguez, partner,*
>
> *SyCip Salazar Hernandez & Gatmaitan, Manila*

In New Zealand, amendments to the privacy act such as mandatory breach reporting are expected. "But there have

certainly been major changes in the way that private corporations do due diligence on external providers of IT and data hosting or processing services, and on any organizations they may partner with in relation to the use of data. Existing obligations under our privacy act, and potential liabilities in contract or tort law, mean that it's vital that an organization ensures that its data hosting and processing services are designed, documented and operated so as to protect the privacy of data subjects," says John Hannan, a partner at DLA Piper New Zealand in Auckland. "'Privacy by design' has become the watchword for organizations where significant value is derived from the collection, use and potential sharing of personal data. Banks and other financial institutions, airlines, and many types of other consumer service providers that collect and rely on data to provide services to consumers."

> "Some work for clients involves assistance provided for building better communication with **government officials so that both** regulator and the regulated speak the same language."
>
> *- Arthur Shay, partner, Shay & Partners, Taipei*

There are significant developments in the Philippines, says Rose Marie M. King-Dominguez, a partner at SyCip Salazar Hernandez & Gatmaitan in Manila. "The National Privacy Commission recently issued rules implementing the 2012 Data Privacy Act. Among other obligations on the part of certain data controllers and processors is a requirement to develop the controller's or processor's personal data processing system and register this with the commission. This is in line with the commission's mandate to ensure compliance with the statute."

In Taiwan, regulations have been slow in responding to increasing cyber attacks, despite the government's continuous emphasis on enterprises' awareness of data protection, says Arthur Shay, a partner at Shay & Partners in Taipei. "Clients approach us for assistance in compliance work for purpose of filling the gap between effective corporate measures and the regulation lagged behind. Some actually involve assistance provided for building better communication with government officials so that both regulator and the regulated speak the same language."

Taiwan's Personal Information Protection Act became effective in 2012 and was amended at the end of 2015. "This has resulted in a substantial increase in compliance-related work, and we expect more enforcement related work in the future," says Chen Hui-ling, a partner at Winkler Partners in Taipei. "The government recently also established the cabinet-level National Center for Cyber Security Technology."

The Thai government is also enacting new legislations and updating the current Computer Crime Act, says Panisa Suwanmatajarn, a senior associate at Siam Premier International in Bangkok. "These draw a lot of attention to our clients and therefore increase our work load."

Expected to be passed by 2017, the Thai Computer Crime Act is being amended to give more powers to enforcement authorities. "Whether or not the amendment will result in an increase of work for a law firm like ours remains a question," says Kowit Somwaiya, a partner at LawPlus in Bangkok. "But personally, I do expect our work on ICT, cyber security, data protection and computer-crime related matters to increase."

In the US, almost every state has been updating its law to ensure that businesses keep customer data as secure as possible, says Alan S. Tilles, chairman of the telecommunications department at Shulman, Rogers, Gandal, Pordy & Ecker in Potomac, Maryland, near Washington. "It has caused a significant increase in work in terms of trying to stay current with more than 40 different state laws which interpret privacy differently. It creates a significant compliance issue for clients, and therefore workload for us in educating our clients."

> "I do expect our work on ICT, cyber security, data protection and computer-crime related matters to increase."
>
> *- Kowit Somwaiya, partner, LawPlus, Bangkok*

In Vietnam, the government efforts are more focused on the youth and censorship, says Steven Jacob, a foreign associate at Indochine Counsel in Ho Chi Minh City. "This is unfortunate because I know at least one hacking incident that originated in Vietnam. The trade is here, but the law is behind."

Outsourcing

Outsourcing information and technology work is now a global trend. "We are seeing many clients doing business with offshore providers. The digital revolution means that national borders can

be quite meaningless in terms of the integration of digital service offering," Hannan says. "This means that assistance with legal compliance, in particular with the data protection and privacy law regimes of various jurisdictions, has to be provided by law firms with global capability."

> "Everyone focuses on IP, but tech issues have, by and large, been tossed by the wayside in Vietnam."
>
> *- Steven Jacob, foreign associate, Indochine Counsel, Ho Chi Minh City*

More and more South Korean companies use cloud services instead of their own or an affiliated company's IT infrastructure. "This is due to the development of cloud as well as the government's promotion of it. In 2015, the National Assembly enacted the Act on the Development of Cloud Computing and Protection of Users. The act exempts certain businesses from the requirement of creating their own IT infrastructure when such operators use cloud," says Jubong Jang, a partner at Lee & Ko in Seoul. "The outsourcing of customer information is also expected to become more commonplace due to the relaxing of consent requirements from customers. When a company outsourced the processing of personal information to a third party, the data subject's consent was almost always required except in certain limited cases. However, such exceptions to the consent requirement have been expanded through recent amendments to related laws and, thus, Korean companies will be able to outsource the processing of personal information more easily."

Another important change which may greatly affect the use of personal information is the South Korean government's recent announcement of new regulatory guidance.

On June 30, 2016, government authorities responsible for enforcing data protection and privacy laws and regulations, including the Ministry of the Interior, the Korea Communications Commission, the Financial Services Commission, the Ministry of Science, ICT and Future Planning, the Ministry of Health and Welfare, and the Office for Government Policy Coordination, jointly announced the Guidelines on Personal Information De-identification Measures and the Comprehensive Guide to Data Protection and Privacy Laws and Regulations.

"By specifying (i) the criteria, procedures, and methods of de-identification measures necessary for utilizing big data, and (ii) the criteria for determining what qualifies as personal information, the Guidelines and the Comprehensive Guide seek to reduce much of the existing ambiguity associated with the concepts of 'personal information' and 'de-identification,' and are laying the foundation for utilizing big data and promoting the security of personal information," Jang says. "Although the Guidelines and Comprehensive Guide do not represent binding legal authority, they may serve to reduce legal uncertainty for companies utilizing de-identified information and such business activities will likely increase Korea's big data market significantly."

"We see many of our multinational clients outsourcing information and technology work. In addition, regional service providers are developing rapidly," Chen says. "This has led to increasingly complex commercial arrangements between data controllers and processors that seek to allocate liability between outsourcers and service providers."

The same thing happens in Thailand. "A number of our clients enter into cloud service agreements and use services of big data centres domestically and internationally. The Board of Investment has enacted regulations that give promotion incentives to local investors/businesses that want to operate data centre services, software creation and software-as-services," Somwaiya says. "The trend has increased our work."

The US faces an identical outsourcing trend, Tilles says. "In some ways, this is great, and it, to some extent, centralizes the number of people responsible for privacy. However, it becomes incumbent on entities to ensure that their outsourcing contracts provide the proper safeguards. The major trend for us is working on these outsourcing contracts to ensure compliance."

"We haven't personally seen much outsourcing in the Vietnamese IT field yet, but we know it's coming," Jacob says. "At a recent conference, we met with an American looking to outsource his programming to Vietnam because it was so much cheaper than in the US."

Rise of the Guardians

While small law firms have been growing for the IT start-up market with lower fees and specialized services in some jurisdictions, they have created zero impact in New Zealand, as it is a global law market with clients operating across borders, says Hannan.

The trend should be welcome from the start-up clients' point of view, as clients would still have quality service with lower costs for most of their daily operations, Shay says. "On the other hand, we see it a good opportunity to move up the food chain in the Taiwan legal market. Clients pay for what they need, and they always do know who in the market would fit their need."

Taiwan's startup scene may still be in its infancy, but it can grow quickly responding to government initiatives such as the previous administration's HeadStart program and the current administration's plans to create an Asian Silicon Valley. "If these plans bear fruit, there could be opportunities for small boutique firms to fill the current mismatch between the specialized needs of startups and the kinds of legal services currently available," Chen says. "We work with several more mature startups, but there is a great need for legal services for early stage startups."

A few law firms/professional firms have launched services to start-ups and SMEs at lower fees in Thailand. Their services centre around "commodity" retail services, Somwaiya says. "Currently they do not affect the legal market but in three to five years, they could negatively impact traditional professional firms, especially if established firms also join them in providing low-cost legal services."

In Vietnam, not that many firms are focusing on the IT sector, Jacob says. "Everyone focuses on IP, but tech issues have, by and large, been tossed by the wayside." AIP