Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia pacific news

Gabriela Kennedy *,[1]

Mayer Brown JSM, Hong Kong

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

ABSTRACT

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

© 2018 Gabriela Kennedy. Published by Elsevier Ltd. All rights reserved.

1. Hong Kong

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

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

1.1. *Droning On – Hong Kong proposes new regulations for drones*

On 3 April 2018, the Civil Aviation Department of Hong Kong ("CAD") launched a 3-month public consultation ("Consultation Paper") on the regulation of unmanned aircraft systems ("UAS").

UASs, more commonly known as drones, have become prevalent for both recreational and commercial purposes globally. Some examples include taking aerial photos and videos at public and private events, carrying out inspections of crops or equipment, conducting search and rescue operations, and even the delivery of packages. However, of course, as with most technology, an increase in popularity leads to an increased awareness of the potential risks associated with UASs, the key concerns of which revolve around personal injury and an invasion of privacy.

1.1.1. *Current regulations*

Under the Air Navigation (Hong Kong) Order 1995 (Cap. 448C) ("Order"), UAS operators must obtain a Certificate of Registration and a Certificate of Airworthiness issued by the CAD ("Certificates") in order to fly a UAS in Hong Kong, unless the UAS weighs no more than 7 kg (without fuel), and will only be used for recreational purposes. UASs that will be used for non-recreational (i.e. commercial) purposes, must obtain the Certificates, regardless of its size or weight. In addition, under the Air Transport (Licensing of Air Services) Regulations (Cap. 448A), any UAS used for hire or reward (e.g. for the provision of photography services, to deliver packages, etc), must apply to the CAD for a permit and comply with any conditions imposed by the CAD ("Permit"). Those that apply for Permits must have in place an insurance policy that covers third party liability for each single UAS operation.

All UASs, irrespective of size or purpose of use, are prohibited from recklessly or negligently causing or permitting a UAS to endanger any person or property. This may amount to an offence.

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

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

https://doi.org/10.1016/j.clsr.2018.04.003
0267-3649/© 2018 Gabriela Kennedy. Published by Elsevier Ltd. All rights reserved.

Recreational UASs that weigh no more than 7 kg (without fuel) are classified as a "flying model aircraft". Whilst exempt from the requirement to obtain the Certificates or Permit, operators are recommended to comply with the CAD's guidelines on the Safety in Radio-Controlled Model Aircraft Flying (15 February 2015). It sets out safety measures for the flying of model aircrafts, e.g. they should not be flown over congested areas, should not fly 300 feet above ground level, and should only be flown during daylight hours.

Reported incidences over the last couple of years on the use of UASs in a manner that posed a risk to the public, have led the government to re-assess the effectiveness of the current regulatory regime. For example, on 2 December 2017, a man was arrested for allegedly flying a UAS over the Formula E racetrack, thereby endangering the personal safety of individuals in breach of the Order. Recreational UASs that are less than 7 kg may still cause damage to property or result in personal injury, yet they are not currently subject to regulation under Hong Kong law.

1.1.2. *Consultation proposal*

Several jurisdictions in Asia have taken up the call to re-evaluate their current regulatory framework to address the evolving use and development of UASs, in order to provide protection where necessary to the public.

In an effort to keep pace, the Hong Kong government commissioned a study in March 2017 on international regulatory practices for UASs with a view to recommending amendments to Hong Kong's current regulatory regime. On 12 March 2018, the Final Report on the Study on the Regulation of UAS in Hong Kong was issued ("Report"). This led to the launch of the Consultation Paper on 2 April 2018. The overall aim of the CAD is to introduce new regulations that protect public safety, without hindering the technological advancements or use of UASs.

Keeping in line with the approach of other jurisdictions, a risk-based approach has been proposed, where regulations that are more stringent apply to UASs that pose a higher risk. In summary, the recommendations put forward in the Report and set out in the Consultation Paper, are as follows:

(1) Establish a UAS registration requirement for UASs over 250 g. Registered UASs should also be labelled with a unique registration number, so that they can be easily identified. This will help ensure that operators are held accountable for any injury or damage caused by their UASs.
(2) Operating standards and requirements should be developed and based on different risk categories of UASs (e.g. based on weight, where it will be operated and how it will be operated), without differentiating between recreational or commercial operations. Currently, 3 main categories are proposed:
    (a) Category A (low risk) – this is further divided into 2 subcategories, i.e. Category A1 for UASs that are 250 g or less, and Category A2 for UASs that are over 250 g but no more than 7 kg. Whilst CAD's approval would not be needed to fly UASs that fall within Category A1, operators must still comply with certain conditions, e.g. must be flown only during the day, and must be flown lower than 100 feet, etc. For Category A2, operators will need to register their UASs with the CAD and will be subject to other requirements, e.g. cannot fly over 300 feet, must be more than 50 metres away from any people or buildings, must have geo-awareness and flight log capabilities, etc.
    (b) Category B (regulated, lower risk) – this will apply to UASs over 7 kg but no more than 25 kg. The UAS would need: (i) to be registered: (ii) to obtain the CAD's authorisation prior to operation; (iii) have geo-awareness and flight log capabilities; and (iv) a safety assessment conducted by the operators.
    (c) Category C (regulated, higher risk) – this will apply to UASs that are over 25 kg, and would impose the most stringent regulations.
(3) Implement training and assessment requirements in light of the different risk categories (the higher the risk, then the more complex the training and assessment).
(4) Developing a UAS map to set out no-fly zones and areas where UASs can be flown.
(5) Prescribe insurance requirements based on the different UAS risk categories. In particular, it is proposed that UASs in Category B or above should be covered by third party insurance.
(6) A further study to be conducted into the indoor operation of UAS.

1.1.3. *Data privacy*

Data privacy concerns have also been a focal point surrounding UAS operations. Whilst the CAD is focused on maintaining aviation safety, the protection of privacy falls within the remit of the Hong Kong Privacy Commissioner.

In Hong Kong, the Personal Data (Privacy) Ordinance ("PDPO") regulates the collection and use of personal data. UASs that can record images or videos may be subject to the PDPO if they seek to collect personal data of the individuals captured. Hong Kong was one of the first jurisdictions in Asia to address specifically data privacy as it applies to UASs. On 31 March 2015, the Privacy Commissioner issued an updated Guidance on CCTV Surveillance and Use of Drones ("Guidance Note").[1]

The practical recommendations relating to CCTV surveillance in the Guidance Note, apply equally to the use of UASs. In brief, operators of UASs need to assess:

(a) whether the use of the UAS is necessary and proportionate to the benefit to be derived from using it;
(b) whether there is a less privacy intrusive method available in order to achieve the same purpose; and
(c) whether it has transparent policies and practices regarding the use of the UAS and any personal data collected, and has adequate measures in place to prevent unauthorised use or access of the UAS or personal data.

[1] http://www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf.

For further details on the Guidance Note, please refer to our previous article entitled "A Brave New World: New Guidance on the Use of Drones Issued in Hong Kong".[2]

1.1.4. *Conclusion*

The public consultation period ends on 3 July 2018. The proposed regulations aim to strike a balance between protecting the public and encouraging the development of UASs. However, whether or not a UAS falls within the scope of the aviation regulations, operators should always remember that they are still subject to the PDPO.

2. Australia

Philip Catania *(Partner), Corrs Chambers Westgarth* (philip.catania@corrs.com.au).

2.1. *Driving into the future: Victoria welcomes driverless cars*

The Victorian Government has passed legislation amending the Road Safety Act 1986 (the "Act")[3] to allow for "automated driving systems" – essentially, trials of technology capable of performing the "dynamic driving task of a motor vehicle".

The legislation establishes the regulatory framework for automated vehicle trials on Victorian highways, clarifying the legal responsibility with these tests and sanctions for not complying with the rules. Based on the permit scheme for human learner drivers, VicRoads is now able to grant permits to individuals or organisations to run a trial of driverless car technology.

This legislation is the latest in a number of legislative regimes created around Australia in the last two years – namely New South Wales and South Australia.

This article sets out the details of Victoria's new regime, and compares this approach to the legislative frameworks established in New South Wales and South Australia.

2.1.1. *How the Victorian regime works*

The Road Safety Amendment (Automated Vehicles) Act 2018 introduced new Part 3A to the Act, establishing a regime for the trialling of automated vehicles on highways ("Victorian Regime").

(a) Application for ADS permit

Under the Victorian Regime, an applicant must apply to VicRoads for an "ADS permit" in relation to a motor vehicle. This application must contain details of the applicant, the vehicle(s), any vehicle supervisor and the nature of the trial.

VicRoads has the powers to require applicants to pass certain appropriate tests or examinations. VicRoads also has broad powers to refuse granting an ADS permits.

(b) ADS permit subject to conditions

When granting an ADS permit, VicRoads can impose certain conditions, including:

- what days the automated vehicle can participate in trials;
- whether a human driver is required to take control of the vehicle at specified times;
- compliance with safety management plans;
- 0% alcohol limit;
- display of "automated vehicle" mark or symbol; and
- real time monitoring of the performance, location and compliance of the automated vehicle.

The ADS permit may remain in force for no more than three years.

(c) Operating a vehicle with an ADS permit

The vehicle supervisor (being a physical person inside a vehicle during a trial) will be held to be "in charge" of the vehicle for the purposes of laws applying to people in charge of vehicles.

Where there is no vehicle supervisor and the vehicle is operating in automated mode, the permit holder of the vehicle is taken to be driving that vehicle. That is, the permit holder will be taken to be in charge of the vehicle when in automated mode.

(d) Offences under ADS Permits

Under the Victorian Regime, it is an offence to:

(i) cause another person to drive or be in charge of automated vehicles where an ADS permit is not in force for that vehicle, or
(ii) drive in breach of any permit condition.

The legislation attaches a significant penalty – $79,285 for a Corporation or $15,857 for individuals – for offences under the regime.

The Victorian Regime also states that the legal burden for any accidents – or complications with the trial – fall on the legal entity responsible for the trial.

2.1.2. *Comparison with South Australia and New South Wales*

South Australia became the first state in Australia last year to pass such laws, requiring organisations to apply directly to the transport minister and meet certain insurance benchmarks.

New South Wales also passed legislation last year which allows the Minister to approve trials – including type of vehicles, roads used and trial time period – and require trial applicants to have the appropriate insurance provisions and safety management plans in place, whilst also allowing for a

[2] https://www.mayerbrown.com/files/Publication/7b583682-7a74-43ce-a26f-e9586d255c07/Presentation/PublicationAttachment/d1d81157-e847-41fa-aa97-f357bbb1d3a5/ASI-IP-TMT-QuarterlyReview-2015Q2.pdf.

[3] http://www.legislation.vic.gov.au/domino/Web_Notes/LDMS/LTObject_Store/ltobjst10.nsf/DDE300B846EED9C7CA257616000A3571/D01CD5BCF6F25F8FCA25824B00069FD0/$FILE/86-127aa182%20authorised.pdf.

two-year driverless bus pilot. Western Australia is currently trialling an electric driverless shuttle buses and autonomous taxis.

3. Malaysia

Charmayne Ong *(Partner), Skrine* (co@skrine.com);
Natalie Lim *(Partner), Skrine* (Natalie.Lim@skrine.com).

3.1. *Think before you speak, think twice before you post*

On 3 April 2018, the controversial Anti-Fake News Bill 2018 ("Bill") was passed in the Dewan Negara and will be sent to the Yang di-Pertuan Agong for the Royal Assent before being gazetted as law. The Malaysian Government reportedly had discussed the draft Bill with various stakeholders including major technology and social media providers such as Google, Facebook, YouTube, Twitter and the Asia Internet Coalition on 12 March 2018 but no public consultation was conducted.

3.1.1. *Why?*

Fake news have always been in existence, spread mostly through word of mouth in ancient times and print ever since printing technology was developed, so why do we need new laws? In recent years, numerous world events have been influenced by fake or inaccurate news; for example, the United States Presidential Election in 2016 was plagued with allegations of fake news influencing the outcome of the election. Fake news did not exist only recently; but they are disseminated much faster and easier today thanks to the Internet and social media.

At home in Malaysia, the Minister has cited the lack of a clear definition of fake news and offences related to social media usage under our existing laws and the limitations of cross-jurisdictional powers as the main reasons for the enactment of the new law. According to Datuk Seri Azalina, the Bill, which identifies the types of offences that can be regarded as spreading fake news, will protect Malaysians from being misinformed and overwhelmed with unverified news. Datuk Seri Najib Razak, the Prime Minister, stated that the Bill was necessary to prevent people from being incited to hate the government or conducting any uprising under the influence of fake news and the Yang di-Pertuan Agong has publicly voiced support for the proposed law on grounds of national stability and security, and also preservation of the values and culture of society.

3.1.2. *What?*

The Bill is comprised of fourteen sections and two schedules. Below are some highlights on the current Bill:

(1) Section 2 of the Bill defines "fake news" as any news, information, data and reports partly or wholly false. Fake news can take any form as long as it is capable of suggesting words or ideas, including features, visuals or audio recordings. Publication of fake news includes electronic publication and written publication.

(2) Section 2 defines "Court" as the Sessions Court, indicating that prosecution will be initiated at the Sessions Court level.

(3) By virtue of Section 3, the Bill has extra-territorial application, signifying that any person (regardless of nationality) whether within or outside Malaysia will be subject to the new law if the fake news concerns Malaysia or affects a Malaysian citizen.

(4) Any person, who maliciously creates, publishes or distributes fake news or publication containing fake news can be liable for a fine of not more than RM 500,000 or be imprisoned for not more than 6 years or both under Section 4 of the Bill. A fine not exceeding RM 3000 per day will be imposed on those who continue to commit the offence after he or she is convicted. Eight illustrations have been included to illustrate certain scenarios where it may or may not be an offence to do certain actions.

(5) Section 5 of the Bill states that those who provide financial aid for the publication of fake news are also liable to the same punishments as stated in Section 4 of the Bill.

(6) Under Section 6, any person who knows or reasonably believes that the publication under his control contains fake news has a duty to remove such publications, failure to do so will result in a fine up to RM 100,000 and a further fine of RM 3000 each day the offence is committed after a conviction.

(7) Section 7 empowers the court to order the removal of fake news and any person affected by the publication can make an ex parte application to the court. Once the court has made such an order, any person not complying with the order can be fined up to RM 100,000. The person affected by the order may apply within 14 days to set aside the order (unless the order relates to a publication containing fake news which is prejudicial or likely to be prejudicial to public order or national security, in which case there shall be no application for the setting aside of such order).

(8) Under Section 8, the police force or any authorized officer under the Communications and Multimedia Act 1998 can be ordered by the Court to remove publications containing fake news, provided that the procedures are followed.

(9) Section 10 provides that any form of abetment that subsequently causes an offence to be committed is subject to the same punishment provided for the offence.

(10) Section 13 provides liability on body corporate. The Director, CEO, manager, secretary or any person responsible for the management of the body corporate can be charged jointly or severally in the same proceedings as the body corporate. He or she shall be deemed guilty of that offence unless it is proven that the offence was committed without his or her knowledge or consent.

3.1.3. *Previous laws in Malaysia?*

Prior to the Bill, the offences relating to the dissemination of false news are found across various existing laws and regulations. For instance, dissemination of false news and information is an offence under Section 8A of the 1984 Printing Presses and Publications Act and Section 233(1) of the

Communications and Multimedia Act 1998. The Sedition Act 1948 also criminalises speeches, whether made orally or in written form, which create hatred, contempt or incite disaffection against the government, promote feelings of ill will and hostility between different races, or question certain provisions of the Federal Constitution. Furthermore, the Official Secrets Act 1972 and the Police Act 1967 also contain certain provisions enacted to ensure national security. Sections 504 and 505(b) of the Penal Code criminalise speech that will cause a breach to public tranquillity, whereas Section 499 criminalises speech that will injure the reputation of another person, dead or alive. The Content Code issued under Section 213 of the Communications and Multimedia Act 1998 also prohibits the dissemination of false content or information. However, the government clearly feels the need to enact new and specific laws on fake news instead of relying on piecemeal legislation. Datuk Seri Azalina claimed that these laws were drafted before or during the 1990s and are barely sufficient to address the nature of the increasingly complex offences that follow rapid technological advancements.

3.1.4. *Conclusion*

The Government has assured that the new law would not be used to control the Internet or restrict freedom of expression. The internet regulator, Malaysian Communications and Multimedia Commission, has also assured that the new law will be enforced equally and fairly.

However, numerous views have already been articulated about the Bill, which has so far been met with controversy. Civil society members have voiced their concerns that the new legislation will further curtail the freedom of speech in Malaysia and pose a threat to journalism. Some groups, including the Malaysian Bar Council, have doubted the necessity of introducing a new piece of legislation as they feel that the existing laws are sufficient to tackle the dissemination of false information or information that places national security at risk. Critics have also pointed out that the definition of "fake news" extends beyond news and covers information not traditionally viewed as news, for example: parody and satire that have a "fake" nature may now be criminalized as "fake news". The impact of the new legislation and how it will be enforced remain to be seen but what is certain is that anyone who uses the Internet and social media will now have to think very carefully before posting or sharing anything.

4. New Zealand

Karen Ngan *(Partner), Simpson Grierson* (karen.ngan @simpsongrierson.com);

Melody Zhou *(Solicitor), Simpson Grierson* (melody.zhou @simpsongrierson.com);

Nick Jens *(Solicitor), Simpson Grierson* (nick.jens @simpsongrierson.com).

4.1. *A new privacy bill*

The Minister of Justice introduced the Privacy Bill to the House on 20 March 2018. The Bill intends to replace the 25-year-old Privacy Act and to bring New Zealand's Privacy laws in line with recent international developments and reforms.

4.1.1. *Key changes*

Fundamental aspects of the Privacy Act, such as the information privacy principles, which regulate the collection, use and disclosure of personal information, are retained, but the Bill introduces new ways to enforce those principles, including more substantive fines and greater powers for the Privacy Commissioner.

The proposed changes include:

- mandatory reporting of privacy breaches;
- compliance notices;
- strengthening cross-border data flow protection;
- new criminal offences;
- the Privacy Commissioner can make binding decisions on access requests; and
- strengthening of the Privacy Commissioner's information gathering power.

4.1.2. *Mandatory reporting of privacy breaches*

An agency must notify the Privacy Commissioner as soon as practicable after becoming aware of a *notifiable privacy breach* (a privacy breach that has caused any type of harm to an affected individual, or there is a risk it will do so). Notice will also need to be given to affected individuals (or to the public).

Failure to comply with these notification requirements is an offence and could result in a fine of up to $10,000.

4.1.3. *Compliance notices*

The Privacy Commissioner will have the ability to issue compliance notices that require an agency to do something, or stop doing something, in order to comply with privacy laws.

The Privacy Commissioner by way of proceedings in the Human Rights Review Tribunal ("Tribunal") may enforce the compliance notice. Equally, an agency may appeal to the Tribunal against all or part of the compliance notice or against the Privacy Commissioner's decision to vary or cancel the compliance notice.

4.1.4. *Strengthening cross-border data flow protection*

New Zealand agencies will need to take reasonable steps to ensure that personal information sent/disclosed overseas will be subject to acceptable privacy standards. Generally, personal information will not be able to be disclosed to an overseas person unless:

- the individual concerned consents to the disclosure of his or her information to the overseas person; or
- the overseas person is in a country that is prescribed in regulations as having privacy laws comparable to New Zealand; or
- the agency believes that the overseas person is required to protect the information in a way that, overall, is comparable to the protections afforded by our New Zealand legislation (e.g., there is an agreement where the overseas person will provide such comparable safeguards).

4.1.5. *New criminal offences*

New criminal offences have been introduced under the Privacy Bill. It will be an offence for a person to:

- make or give any false or misleading statements or information to the Privacy Commissioner or other persons exercising powers under the Privacy Act;
- falsely represent that he or she has authority under the Privacy Act;
- impersonate or falsely pretend to be an individual for the purposes of obtaining access to that individual's personal information or having that individual's personal information used, altered or destroyed; and
- knowingly destroy documents containing personal information that is the subject of a request.

Any person that commits any of the above offences will be liable to a fine of up to $10,000.

4.1.6. *Privacy commissioner's binding decisions on access requests*

The Privacy Commissioner will have the power to make binding decisions on complaints relating to access to personal information (instead of the current process where the Privacy Commissioner refers such complaints to the Tribunal). In particular, if an agency refuses an individual's request to access his/her personal information, the Privacy Commissioner will be able to direct that agency to make that information available.

Agencies will have the ability to appeal to the Tribunal against a decision by Privacy Commissioner to make the information available.

4.1.7. *Privacy commissioner's information gathering power*

The Privacy Bill will strengthen the Privacy Commissioner's existing investigation powers by allowing the Privacy Commissioner to shorten the time frame within which an agency must comply and increasing the penalty for non-compliance.

4.1.8. *What's next?*

From here, the Privacy Bill will have its first reading in Parliament and then be referred to the Select Committee where a round of public consultation will take place and further amendments might be included.

4.2. *Review of the search and surveillance* Act 2012 ("Act")

The New Zealand Law Commission ("Commission") and the Ministry of Justice ("Ministry") have together, released a joint report on the Review of the Search and Surveillance Act 2012 five years after the commencement of that Act ("Report").

4.2.1. *Objective of the review*

The terms of reference for the review required consideration of the Act and to determine whether any amendments are necessary or desirable. The objective was to ensure that the Act provides for effective law enforcement and maintains consistency with human rights laws, now and into the future, in light of developments in: technology; case law; and international practices.

The Report notes that although there are some areas of the Act that would benefit from clarification, and some that could be updated to reflect international trends, a major overhaul was not required. However, two wider problems were identified:

- key aspects of search and surveillance law are contained in case law and not currently reflected in the Act; and
- the Act has not kept pace with developments in technology.

4.2.2. *Case law*

The Report records the recommendation that the Act be amended to include a provision setting out principles that are based on case law, and assist decision making as to when and how search powers are exercised under the Act. The Report sets out seven recommended principles, three of which seek to address privacy concerns.

4.2.3. *Technology issues*

The Report notes that the Act has not kept pace with developments in technology. In particular:

- the volume of data stored in electronic form has grown exponentially;
- electronic devices are sophisticated and are used globally;
- it is becoming common to store data in the Cloud; and
- encryption and anonymisation tools are being used more frequently.

The Commission and the Ministry also noted that developments in technology have heightened the public's interest in the privacy of their information, and the need to observe individuals' privacy rights.

Some of the recommendations that address the development of technology are:

(1) Allow surveillance warrants to be issued for surveillance technology as opposed to surveillance devices, in recognition of the fact that surveillance can be carried out using intangible technologies (such as computer programs rather than devices).
(2) Allow for the use of keystroke technology to assist enforcement officers in obtaining passwords and encryption keys to gain access to electronic devices. In addition, clarifying that the privilege against self-incrimination can be used to refuse to provide access information for a device only in very limited circumstances.
(3) Allow a warrantless search power to seize and secure, but not search, an electronic device (such as a smart phone). Search of an electronic device would still require a search warrant.
(4) Provide for internet searches – that is, search of data that is accessible from a device using the internet and that is stored in New Zealand or an unknown location. It has been noted that the Act needs to recognise how frequently information that could be stored on a device is now stored on the cloud. However, it has also been noted that this is a challenging area.

4.2.4. *What's next*

The Government is to consider whether the Report's recommendations should either be:

(1) accepted in whole, or part, and draft a Bill amending the Act accordingly; or
(2) Rejected, and make no amendment to the Act.

However, no time frame is prescribed by statute; nor has the Government indicated when it will make comment on the Report.

5. Singapore

Lam Chung Nian *(Partner), WongPartnership LLP* (chungnian.lam@wongpartnership.com);
Zhao Feng Quek *(Practice Trainee), WongPartnership LLP* (zhaofeng.quek@wongpartnership.com).

5.1. *Singapore joins APEC data privacy system*

On 6 March 2018, Singapore joined both the APEC Cross-Border Privacy Rules ("CBPR"), and the Privacy Recognition for Processors ("PRP") systems. Both systems are certified multilateral certification mechanisms that ensure that certified organisations have in place data protection policies that are consistent with the APEC Privacy Framework (the "Framework").[4]

Certified companies in Singapore will be able to exchange personal data with other certified companies in participating APEC economies seamlessly. The certification also means that consumers can be assured that the cross-border transfer of their personal data will be subject to high standards of data protection. The Ministry of Communications and Information has indicated that the Personal Data Protection Commission is working on the certification scheme and companies can start applying for the CBPR and PRP systems certification in 2019.

By way of background:

- The Framework is comprised of a set of guiding principles to assist APEC economies in developing consistent domestic approaches to personal information privacy protection, and forms the basis for the development of a regional approach to promote accountable and responsible transfers of personal information between APEC economies.
- The CBPR System is a product of a cooperative project among participating APEC economies to develop a simple, transparent system usable by organisations (personal information controllers) for the protection of personal information moving across APEC economies.
- The PRP System, on the other hand is a recognition system for personal information processors, including organisations that process data on behalf and on instruction of other organisations. The PRP System was designed not only to help processors demonstrate their capacities for processing of personal information in general, but also to assure that the said processing is at least consistent with the controller's applicable requirements for processing under a CBPR system.
- Both the CBPR and PRP Systems do not displace or change an APEC economy's domestic laws and regulations, nor displace a participating organisation's domestic legal obligations. Where domestic legal requirements exceed what is expected in the PRP System, the full extent of such domestic law and regulation would continue to apply.

The CBPR System consists of four broad elements[5]:

- *Self-assessment*: A self-assessment of an organisation's data privacy policy and practices is conducted by the APEC economy against the requirements of the APEC Privacy Framework using an APEC recognized CBPR questionnaire;
- *Compliance Review*: The completed questionnaire and any associated documentation will then be submitted to an APEC-recognized Accountability Agent[6] for confidential review for compliance with the standards established in the CBPR programme requirements;
- *Recognition/Acceptance*: APEC economies will establish a publicly accessible directory of organisations that have been certified as compliant with the CBPR Systems, with contact and business details of compliant organisations maintained; and
- *Dispute Resolution/Enforcement*: Accountability Agents and privacy enforcement authorities will have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with CBPR program requirements.

The PRP System also operates by way of the same four broad elements resembling the CBPR Framework, the difference being that the compliance questionnaire, review, recognition/acceptance, and dispute resolution elements are all instead based on the PRP System requirements.[7]

Singapore is the sixth APEC economy to participate in the CBPR system alongside USA, Mexico, Canada, Japan and the Republic of Korea, and the second APEC economy to participate in the PRP system alongside the USA.

5.1.1. *Comments*

Singapore joining the APEC CBPR and PRP systems reflects its intentions to facilitate interoperability between different privacy regimes, and reduce barriers to digitally based trade. Adoption of the CBPR and PRP systems among organisations could also aid in promoting greater trust among organisations and consumers online. Whilst the application of the systems is currently limited to six economies, there has also been a meeting between the APEC Electronic Commerce Steering Group and the European Commission in August 2017 to begin discussions

[4] In November 2004, Ministers for the 21 APEC economies endorsed the APEC Privacy Framework.

[5] *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines*, [9] (See: https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf, [9].

[6] An APEC economy may recognize an Accountability Agent through defined procedures under the CBPR and PRP systems. An Accountability Agent's primary roles are to review an organisation's data protection and privacy policies for compliance with the respective CBPR and PRP System, and to enforce the said organisation's compliance with the CBPR or PRP program requirements.

[7] *APEC Privacy Recognition for Processors System*, [4]–[24] See: https://www.apec.org/~/media/Files/Groups/ECSG/2015/APEC%20PRP%20Rules%20and%20Guidelines.pdf.

on recognizing the CBPR System as a certification under the EU's General Data Protection Regulation.

However, as an organisation's participation in the CBPR and PRP systems is voluntary, Singapore's membership of the CBPR and PRP schemes does not mean that the benefits of the schemes will be automatically realised. Whether an organisation will self-certify under the CBPR and PRP systems will also depend on the nature of the organisation's business, and whether the organisation considers such certification is vital having regard to its customers and business partners. Programmes encouraging wider adoption of the CBPR and PRP schemes may be required for organisations readily to adopt participation in these schemes, and for the objectives of the schemes to be achieved.

5.2. *Data protection and the law of privacy*

The Personal Data Protection Commission ("PDPC") has in a decision dated 12 February 2018 invoked for the first time its powers to discontinue investigations under Section 50(3) of the Personal Data Protection Act ("PDPA"). The case in question concerned a complaint to the PDPC made on 5 November 2016 by an individual ("Complainant") against a company in the business of selling digital locks ("Organisation").[8] Specifically, the complaint concerned the Organisation's uploading of a police report ("Report") to social media, which alleged that the Complainant was harassing the Organisation's staff.

The Deputy Commissioner ("DC") invoked his jurisdiction to discontinue investigations, holding that the crux of the dispute went beyond the domain of the PDPA (which was confined to the regulation of the management and protection of personal data).

The DC clarified that although the common law does not recognise a general right to privacy, a framework of common law actions and statutory torts exist that collectively protect various aspects of an individual's privacy. In view of this, it would have been a mistake to distort the PDPA, which dealt with informational privacy, in order to address privacy issues that it was not meant to cover – issues which would have been better addressed by other laws in the Singapore legislative framework or under the common law.

5.2.1. *Facts*

This case concerned the Complainant's third complaint against the Organisation, the first two complaints concerning two separate instances of unwanted disclosure of the Complainant's personal data by the Organisation on: (i) Facebook; and (ii) the blog of the Organisation's sole director respectively. This third complaint concerned a Facebook post that the Organisation's staff had posted which contained inter alia, the Report.

The DC, in his decision to exercise his discretion to discontinue investigations and issue an advisory notice to the Organisation, offered clarification on the following points:

- Whether an unauthorized disclosure or access of information about an individual in a document ought to be one that requires scrutiny under the PDPA; and
- How the PDPA sits within the framework of statutory and common law rights that collectively provide safeguards to the privacy of individuals in Singapore.

5.2.2. *Ambit of the PDPA'S application*

The DC clarified that the PDPA's scope only applied to documents concerning personal data,[9] which required the preliminary consideration as to whether the document was "clearly about an individual or individuals". Such a consideration involved a two-pronged assessment where the Commissioner would:

(1) first consider whether the document is clearly about an individual or individuals; and
(2) second, where the document is not clearly about an individual, consider whether the information is "biographically significant".[10]

The DC considered that social media posts (as in the present case) could contain biographically significant information in the form of identifiers (i.e. who authored the posts), even if the purpose of such messages was not to convey such information. As the Report concerned harassing conduct purportedly carried out by the Complainant in name, the disclosure of the Complainant's identity was therefore one of the purposes of the report, and potentially of biographical significance.

The DC also reiterated that individuals have two avenues through which they could address concerns of an organisation's potential breach of the PDPA, either by:

(1) submitting a complaint to the Commission; or
(2) where the individual has suffered loss or damage directly as a result of the contravention, by commencing civil proceedings against the organisation.[11]

The DC considered that the Commissioner's discretion under the PDPA[12] to suspend, discontinue, or refuse to discontinue an investigation only came into play in the case of the first avenue. Such discretion could be exercised in situations where the severity of the potential breach did not warrant any further action, considering factors such as the nature of the personal data affected, the number of people affected, whether the

[8] *My Digital Lock Pte Ltd* [2018] SGPDPC 3 (see: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/MyDigitalLockGD2018-02-09.pdf).

[9] Section 2 of the PDPA: "personal data" means data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the association has or is likely to have access.

[10] Information is "biographically significant" where the focus of the information is on the data subject, or some transaction or event in which the data subject may be figured or had an interest in. The recording of the information goes beyond the mere "putative data subject's involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised". (*see Durant v Financial Services Authority* [2003] EWCA Civ 1746, at [28]).

[11] Section 32 of the PDPA.

[12] Section 50(3) of the PDPA.

breach was due to systemic issues, and the likely effect on the individuals concerned.

The DC clarified that these considerations were not exhaustive, and other aspects of the discretion would be explained within the factual matrices of future cases.

5.2.3. *The PDPA's interaction with statutory and common law rights*

Notwithstanding that the information in a document published in an unauthorized manner was clearly about, or biographically significant pertaining to an individual (thus falling within the ambit of the PDPA), the DC clarified that it was not always the case that the PDPA necessarily offered the most appropriate remedies.

On the facts, the DC was of the view that the true nature of the Complainant's claim was concerned with the protection of his privacy or reputation, which extended beyond the protection of his personal data. In an assessment of the applicable law concerning the protection of an individual's privacy in Singapore, the DC came to the following conclusions:

(1) though the common law does not recognise a general right to privacy, a framework of common law actions and statutory torts exist that collectively protect various aspects of an individual's privacy;
(2) such aspects included: (i) the right to seclusion[13]; (ii) the right to prevent publication of private communication[14]; (iii) the right of publicity[15]; and (iv) the right to prevent false light publicity[16]; and
(3) given that the law provided existing options to protect the privacy or reputation of the Complainant (such as the law of defamation, or the statutory tort of intentional harassment[17]), it would have been a mistake to distort the PDPA, which dealt with informational privacy, in order to address privacy issues it was not meant to cover.[18]

5.2.4. *Additional comments by the DC*

The DC, in coming to his decision, also gave the following additional comments:

- an organisation could not always be prevented from defending itself on the same public forum where a Complainant chose to ventilate its dissatisfaction. Disclosure of personal data would in some occasions be necessary, and the matter would only be investigated under the PDPA where such disclosure was a disproportionate one;
- on the facts of the case, the disclosure of the Complainant's name was not a disproportionate one;
- considering the history between the Complainant and the Organisation, resolution of the dispute by the PDPC was unlikely to resolve the underlying dispute between them; and
- the history of exchanges between all relevant parties disclosed issues that would have been better addressed before court proceedings, such as the Complainant's expectation of privacy and alleged reputational damage.

5.2.5. *Comments*

This case represents the first time the PDPC has invoked its discretion under Section 50 of the PDPA to discontinue investigations. The decision sheds light on the specific considerations of the PDPC in making such a decision, encompassing the interplay between the legislative ambit of the PDPA and other remedies in statutory and common law. It is clear that the PDPC considered that in certain factual scenarios, the PDPA might not be a suitable remedy for disputes dealing with a breach of privacy or reputational rights, as the PDPA deals more with "informational privacy". In such cases, the law of defamation or the statutory tort of intentional harassment may be more appropriate. It remains to be seen if future decisions will add further colour to the distinction between privacy rights and "informational privacy".

[13] This right concerns an individual's right against invasion of his private space or affairs.
[14] This right concerns the right to prevent a misuse of private information, or a wrongful disclosure of personal information.
[15] This right concerns an individual's right to control the commercial exploitation of his or her fame or identity.
[16] This right concerns the need to protect the reputation of the individual from publicity that places the individual in a false light.
[17] Sections 3 and 4 of the Protection from Harassment Act (Cap. 256A).
[18] Sing., *Parliamentary Debates*, vol. 89 (15 October 2012) (Assoc Prof Dr Yaacob Ibrahim) at p. 41.