ABA Antitrust Law 2019 Spring Meeting
Thursday, March 28, 2019

RESHAPING PRIVACY REGULATIONS: COMPLIANCE AND CONSEQUENCES

Session Chair: **Katherine ARMSTRONG, Drinker Biddle & Reath LLP, Washington, DC**

Moderator: **William C. MACLEOD, Kelley Drye & Warren LLP, Washington, DC**

Speakers: **Ruth BOARDMAN, Bird and Bird LLP, London**

Pam DIXON, Executive Director, World Privacy Forum, Portland

Rebecca K. SLAUGHTER, Commissioner, Federal Trade Commission, Washington, DC

Stephen Kai-yi WONG, Privacy Commissioner for Personal Data, Hong Kong, China

Grooving Privacy Evolution with Law Reform and Data Ethics

by Stephen Kai-yi WONG, Barrister, Privacy Commissioner for Personal Data, Hong Kong, China

Table of Contents

1. Personal Data Protection in Hong Kong

The data protection law of Hong Kong – the Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong Kong (**PDPO**[1]) – was the first comprehensive data protection law in the region when it was enacted in 1995 with reference to the OECD Privacy Guidelines 1980 and the draft EU Data Protection Directive 1995. It was noticed in the early 1990s that an increasing number of jurisdictions had enacted data protection laws commensurable to the OECD Privacy Guidelines 1980, and the lack of information privacy regime in Hong Kong was hindering the flow of data to the city because the legislation of these jurisdictions often prohibited the flow of data to another jurisdiction which did not provide for adequate data protection[2]. In the circumstances, it was considered necessary to give internationally agreed data protection standards statutory force in Hong Kong in order to discharge Hong Kong's obligation in human rights protection and retain Hong Kong's status as an international trading centre[3].

The PDPO has created an independent regulator, i.e. the Privacy Commissioner for Personal Data (**PCPD**). The PCPD regulates both the private and public (including the government) sectors. In addition to law enforcement, the PCPD has the statutory function to promote awareness and understanding of, and compliance with the PDPO[4]. With relentless education and promotion, the PCPD witnessed an increasing public awareness on personal data protection in Hong Kong. Today, we can hardly live a day in Hong Kong without seeing privacy-related stories in the local newspapers. The number of data breach notifications received by the PCPD is on the rise, despite the fact that the notifications are on voluntary basis. Organisations are keener to practise privacy accountability and data ethics.

---

[1] Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong Kong: https://www.elegislation.gov.hk/hk/cap486

[2] The Law Reform Commission of Hong Kong, "*Reform of the Law Relating to the Protection of Personal Data*" (August 1994), paragraph 17.9: https://www.hkreform.gov.hk/en/docs/rdata-e.pdf

[3] The Law Reform Commission of Hong Kong, "*Reform of the Law Relating to the Protection of Personal Data*" (August 1994), paragraph 5.2: https://www.hkreform.gov.hk/en/docs/rdata-e.pdf

[4] Section 8(1) of PDPO: https://www.elegislation.gov.hk/hk/cap486?xpid=ID_1438403261271_001

2. The Digital Revolution

Extensive and ubiquitous collection of personal data, both online and offline, together with the unpredictability in the use and transfer of the data, have challenged global data privacy frameworks around the world which are essentially based on 'notification' and 'consent'. Often, individuals are not even aware that their personal data has been collected or shared, let alone having the ability to exercise control over their data or objecting to unfair or discriminatory use of it.

Personal data does not belong to any organisation, but to the individuals from whom the data is collected. Individuals ought to be entitled to have the control, or self-determination, over it – "Personal Data in Our Hands" as we put it. This is principally what is enshrined in Hong Kong's PDPO and affirmed by the EU General Data Protection Regulation (**GDPR**).

On the other hand, in this data-driven economy that keeps growing in parallel with the advent of big data and ICT developments – from which we benefit tremendously – it would not be in the interest of the community to have data locked up. One of the challenges that the PCPD, as a regulator, has to face in the Age of Artificial Intelligence and Big Data, is how the PCPD can help unlock and share personal data within the legal and ethical frameworks, with a view to maximising the benefits of data in a sustainable way, minimising the risks and harms, creating healthy synergy with economic growth, and securing the innovative use of personal data.

In Hong Kong, the use of data technology by both the public and private sectors has become increasingly prevalent. In late-2017, the Government published the "Hong Kong Smart City Blueprint" setting out policy objectives to pursue smart city development by making use of innovation and technology. Key initiatives in the Blueprint include encouraging open data and using data analytics to improve public services. The Government also aims at developing new economic pillars by building a data hub and advanced manufacturing centre within the next few years. Adoption of technologies like artificial intelligence, blockchain, cloud computing and data analytics is also on the rise worldwide, in both the private and public sectors.

3. Recent Regulatory Developments

3.1 The OECD Guidelines and APEC Framework

Since the mid-1970s, the OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. For a long time, the 1980 OECD Privacy Principles provided a commonly used privacy framework internationally – reflected in existing and emerging privacy and data protection laws around the world, including that of Hong Kong. They contained eight fundamental data protection principles, i.e., collection limitation, data quality, purpose specification, use limitation, data security safeguards, openness, individual participation (e.g., right to access personal data) and accountability[5].

In 2013, the OECD Council adopted its first update to its Guidelines. Data security breach notification was one of the new concepts introduced. The two themes that ran through the updated Guidelines were a focus on the practical implementation of privacy protection through an approach grounded on **risk management**, and the need to address the global dimension of privacy through **improved interoperability**[6].

In the Asia-Pacific region, the APEC Privacy Framework was first adopted by the APEC member economies in 2005. It aimed at promoting e-commerce in the Asia-Pacific region, and was consistent with the core values of the 1980 OECD Principles. It contained nine principles, and articulated in express terms the principles of notice, choice (i.e. consent) and the rights of data access and data correction[7].

In 2015, an update to the APEC Privacy Framework was adopted. The 2015 Framework drew upon concepts introduced into the 2013 OECD Revised Guidelines, taking into consideration the different legal features and context

[5] 1980 OECD Guidelines and the 8 Privacy Principles: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2

[6] 1983 OECD Revised Guidelines (2013): http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[7] APEC Privacy Framework 2005: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework

of the APEC region. The 2015 Framework specifically addresses the importance of protecting privacy while maintaining information flows – recognising that business operations and consumer expectations have undergone major shifts resulting from the emergence of digital economies[8].

3.2 The EU Directive and the GDPR

The 1995 EU Data Protection Directive [9] was an early piece of comprehensive privacy law which set down the model legal concepts for all European national laws for many years. In fact, the 1980 OECD Privacy Principles and the 1995 EU Data Protection Directive are sometimes regarded as the first and second generations of data protection standards respectively.

In 2016, the national data protection laws of the 28 member states (made pursuant to the Data Protection Directive) were harmonised into a single set of EU privacy law – the GDPR – directly applicable to all member states. The GDPR came into force in May 2018.

The GDPR is considered by some academics and data protection practitioners as the third generation of data protection law[10]. It was written with the emerging technologies of profiling and automated decision making in mind. It aims at returning control of personal data to individuals to whom the personal data belong, and imposing greater accountability on data controllers, having considered the possible impact of data processing on the interests, rights and freedoms of consumers.

The major changes brought by the GDPR include enhancements to many concepts already existent under the 1995 EU Data Protection Directive, as well as new requirements:

---

[8] APEC Privacy Framework 2015:
https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)
[9] EU Directive 95/46/EC:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en
[10] Graham Greenleaf, "*European data privacy standards implemented in laws outside Europe*", 21 [2018] UNSWLRS 2: http://classic.austlii.edu.au/au/journals/UNSWLRS/2018/2.html

- the rules on **extra-territorial application** have been enhanced – in recognition of the global nature of data flows not limited by national borders;
- express recognition of **accountability** as a guiding paradigm in data protection – as exemplified in new emphasis on appointments of Data Protection Officers, mandatory data breach notifications, and promotion of trust seals and certifications;
- **enhanced rights for data subjects**, particularly regarding data erasure and protection against automated decision-making.

Although the GDPR was designed to regulate Europe, it has been a catalyst for law reforms outside Europe since its passage in 2016[11]. It has generated waves of legislative reforms and debates on proposed reforms around the world, including in the mainland and Hong Kong Special Administrative Region of China.

3.3 Data Protection Developments in Neighbouring Jurisdictions

(a) The Mainland of China

The concept of privacy is virtually non-existent in China's traditional culture. However, the concept of privacy right has slowly emerged in the mainland of China as it underwent the economic reform and urbanisation in the late 20th century, with its people calling for greater privacy protection[12]. In the recent decade, authorities in the mainland of China have been catching up fast and working hard putting in place data protection measures. For example,

- the 2nd Amendment to the Law on the Protection of Consumers' Rights and Interests enacted in November 2013 requires an operator

[11] Elizabeth Denham's speech to the International Privacy Forum (4 December 2018): https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/12/international-privacy-forum-forum/

[12] Li-ming Wang, "*Privacy Protection in China: Paths, Characteristics and Issues*", a paper for the 39th International Conference of Data Protection and Privacy Commissioners held in Hong Kong in September 2017 (pages 90-91): https://www.privacyconference2017.org/eng/files/programme_booklet.pdf

who provides goods or services to consumers to obtain the consumers' consent and abide by the principles of legality, propriety and necessity when collecting and using the consumers' personal information, as well as to protect the confidentiality of the information[13];

- the 9th Amendment to the Criminal Law implemented in November 2015 makes it a criminal offence for provision or sale of personal information in breach of the country's regulations. An offender is punishable by imprisonment and fine[14];
- the Cybersecurity Law 2017, which came into force in June 2017, provides quite comprehensive, albeit broad-brush, regulation on the processing of personal information by network operators, such as the principles for collection and use of personal information, obligation on data security and data breach notification, and individuals' rights to correction and deletion of personal information [15]. The Cybersecurity Law strengthens the data protection regime in the mainland of China;
- the General Provisions of the Civil Law, which came into effect in October 2017, formally recognises individuals' rights to privacy and personal information protection. Pursuant to the General Provisions, an individual may file a claim in tort if his privacy or personal information right has been infringed; and
- the E-Commerce Law implemented in January 2019 requires e-commerce operators to provide non-personalised goods/services recommendations to individuals when personalised recommendations are provided[16].

In May 2017, the Supreme People's Court and the Supreme People's Procuratorate jointly issued an interpretation on several issues concerning the application of law in the handling of criminal cases of infringing on citizens' personal information, such as the definition of "citizen's personal

[13] Article 29 of the Law on the Protection of Consumers' Rights and Interests (in Chinese): http://www.npc.gov.cn/npc/xinwen/2013-10/26/content_1811773.htm
[14] Article 253(1) of the Criminal Law of the mainland of China (in Chinese): http://www.npc.gov.cn/npc/xinwen/2015-08/31/content_1945587.htm
[15] Articles 40-45 of the Cybersecurity Law (in Chinese): http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm
[16] Article 18 of the E-Commerce Law (in Chinese): http://www.npc.gov.cn/npc/xinwen/2018-08/31/content_2060172.htm

information", and the meanings of "in breach of the country regulations" and "serious situation" under the Criminal Law[17]. The interpretation is intended to provide certainty to the application of the laws in personal information-related cases.

The provisions relating to personal information protection under various laws of the mainland of China are generally broad-brush and principle-based. The Personal Information Security Specification was therefore implemented in May 2018 to provide detailed guidance and bridge the gap between the legal requirements and the business practice. The Specification itself is not legally-binding. However, some academics and legal practitioners' in the mainland of China believe that non-compliance with the Specification may be considered as a breach of a relevant provision in the aforesaid law.

In December 2018, the State Council of the PRC issued a White Paper entitled "*Progress in Human Rights over the 40 Years of Reform and Opening Up in China*". In the White Paper, the State Council reiterated the Government's commitment to respecting and protecting human rights enshrined in the Constitution, which includes the rights to personal dignity and privacy of correspondence.

Most notably, in September 2018, the Standing Committee of the National People's Congress listed the Personal Information Protection Law in its legislative agenda, under Category 1. It indicates that the conditions for legislation are mature and the relevant bill will be deliberated by the Standing Committee within its current 5-year term.

A civil case at the First Intermediate People's Court of Beijing in 2017 provided a glimpse of how the personal information right was protected in the mainland of China[18]. In that case, the plaintiff, shortly after he had booked a flight ticket through an online travel agent, received a fraudulent text message through his mobile phone, alleging that his flight had been

[17] Interpretation of the Supreme People's Court and the Supreme People's Procuratorate (in Chinese):
http://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml
[18] Press release by the First Intermediate People's Court of Beijing, 27 March 2017 (in Chinese):
http://bj1zy.chinacourt.org/article/detail/2017/03/id/2633821.shtml

cancelled. In the message, the plaintiff was also asked to follow up by dialling a number provided. The plaintiff, having realised that the message was fraudulent, sued the online agent and the airliner for leaking his personal data. The plaintiff lost at the first trial because he was unable to prove that the personal information used by the fraudsters derived from the defendants. The plaintiff succeeded on appeal at the First Intermediate People's Court, which ruled that it was wrong to require the plaintiff to prove the source of the personal information. Having considered the sequence of the events, the fact that the defendants possessed the leaked information and some other factors, on balance of probabilities, the Intermediate Court was satisfied that the defendants were liable for the data leakage. As a remedy, the Intermediate Court ordered the defendants to publish an apology to the plaintiff on their websites. The plaintiff's claim for damages was nevertheless rejected by the Intermediate Court because he was unable to prove injury to his feelings. This case is important for two reasons: first, it acknowledges the difficulty of a plaintiff in proving the source of his/her personal information being misused and lays down a lower threshold for the plaintiff to establish a claim; second, it reaffirms the courts' long-standing stance that proof of injury is required in order for the plaintiff to obtain damages[19].

(b) Macao, China

The Personal Data Protection Act of Macao (Law no. 8/2005) came into force in 2006. The Act largely modelled on the Portuguese data protection regime (Law no. 68/98), which is in turn transposed from the 1995 EU Data Protection Directive.

In October 2018, the Legislative Assembly of Macao approved the Cybersecurity Law. The Cybersecurity Law was intended to become operational in six months after approval. The Cybersecurity Law mainly applies to public sectors' networks and data systems, as well as to the private entities that operate critical infrastructures in Macao, such as transportation, telecommunication, banking and insurance, medical affairs, electricity and water supply. Regulated entities are required to implement

[19] Chen Chen and Li Si-di, "*Breakthrough and predicament in legal protection of personal information*", Legal Weekly, 23 January 2019 (in Chinese): http://www.legalweekly.cn/article_show.jsp?f_article_id=17830

organisational, procedural, preventive and remedial measures to ensure the security of systems and networks, appoint managers to oversee network security, and report to the regulatory bodies in the event of security incident, among others.

(c) Japan

Japan enacted a data protection law to regulate computer processing of personal data by administrative organs in 1988. It was the first data protection law of its kind in Asia. In 2003, the Act on the Protection of Personal Information (**APPI**) was promulgated to regulate processing of personal data by the private sector. The regulatory regime of data protection in Japan had been fragmented until the APPI was amended in 2015 and came into effect in May 2017. The Amended APPI established the Personal Information Protection Commission to centralise the regulatory power over the handling of personal information by business operators[20]. Other notable changes in the Amended APPI include the restrictions on cross-border transfer of personal information and extra-territorial application of the law[21].

In January 2019, Japan and the EU announced that they had adopted mutual adequacy decisions in respect of personal data transfers between the two jurisdictions. After putting in place additional safeguards to complement the existing law, Japan and EU together recognised that data transfers between them mutually enjoy a commensurate level of legal protection.

Some of the measures that Japan has put in place in order to obtain the adequacy status from the EU include[22]:

---

[20] Masao Horibe, "*Privacy Culture and Data Protection Laws in Japan*", a presentation at the 39th International Conference of Data Protection and Privacy Commissioners held in Hong Kong in September 2017:
https://www.privacyconference2017.org/eng/files/ppt/masao_horibe.pdf

[21] DLA Piper - Data Protection Alert, *Update on amendments to Japan's privacy law*, 19 January 2017:
https://www.dlapiper.com/en/hongkong/insights/publications/2017/01/update-on-amendments-to-japans-privacy-law/

[22] European Commission - Press release, *European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows*, 23 January 2019:
http://europa.eu/rapid/press-release_IP-19-421_en.htm

- a set of Supplementary Rules that bridge several differences between the two data protection systems (e.g., strengthening the protection of sensitive data and the conditions for onward transfers of EU data from Japan to another third country);
- the Japanese government's assurance to the European Commission that government access of data for law enforcement and security purposes would be limited to what is necessary and proportionate, and subject to independent oversight and effective redress mechanisms; and
- a complaint-handling mechanism to address complaints from Europeans regarding access to their data by Japanese authorities, to be administered by the Personal Information Protection Commission of Japan.

(d) Singapore

When the Singapore's Personal Data Protection Act was enacted in 2012, a lot of guidance was taken from the OECD Guidelines and the Canadian data protection law[23]. Considering the challenges of new data processing technologies, like Internet of Things and artificial intelligence, and other factors, the Personal Data Protection Commission of Singapore has been working on reforming its law and its regulatory strategy.

Two years ago, the Personal Data Protection Commission embarked on a process to help organisations in Singapore to transform from compliance to accountability for the purpose of building trust with consumers in the digital economy. One initiative for the accountability programme is the Data Protection Trust Mark launched in January 2019. The Trust Mark serves as a visible badge of recognition of an organisation that has demonstrated accountability and responsibility in data protection policy and practice.

Currently, two amendments to the Personal Data Protection Act 2012 are in the pipeline: one is enhancing the consent regime; the other is mandatory

[23] Leong Keng Thai, Keynote Speech at the Peking University Law School & Development Academy on 15 January 2019: https://www.pdpc.gov.sg/News/Press-Room/2019/01/Keynote-Speech-at-Peking-University-on-15-January-2019

breach notification. Under the enhanced consent regime, an organisation would be allowed to use personal data for new purposes by either (i) notifying the individual data subjects, or (ii) demonstrating the legitimate interest of the new uses, if certain conditions are met.

(e) The Philippines

The word "privacy" does not translate into any of the eight major languages in the Philippines. Nonetheless, privacy is heavily protected in the country's constitution partly because of more than a decade of authoritarian rule in the past[24].

The Data Privacy Act of 2012 of the Philippines came into force in March 2016 upon the establishment of the National Privacy Commission. Just like the APEC Privacy framework, the Data Privacy Act highlights the free flow of information to foster innovation while protecting personal information[25].

Recently, the National Privacy Commission has been advocating a shift from compliance to accountability in personal data protection, as well as a shift from consent to legitimate interest as the basis of data processing, having noticed that consent has become a mere default and "consent fatigue" has started to set in[26]. In December 2018, the Commission took one step further in promoting accountability and data ethics by unveiling its DPO Accountability, Compliance, and Ethics (**ACE**) Programme. The ACE Programme aims at establishing a skills benchmark for local privacy professionals and preparing them to embrace ethical data processing, which is crucial for building trust in the digital world[27].

---

[24] Raymund Liboro, "*Data Protection in the Philippines*", a paper for the 39th International Conference of Data Protection and Privacy Commissioners held in Hong Kong in September 2017 (page 96):
https://www.privacyconference2017.org/eng/files/programme_booklet.pdf

[25] Ditto

[26] Manila Bulletin, "*NPC seeks to tighten personal data protection*", 19 August 2018:
https://business.mb.com.ph/2018/08/19/npc-seeks-to-tighten-personal-data-protection/

[27] National Privacy Commission of the Philippines, "*NPC launches DPO ACE Program, sets benchmark for data privacy training in PH*", 12 December 2018:
https://www.privacy.gov.ph/2018/12/npc-launches-dpo-ace-program-sets-benchmark-for-data-privacy-training-in-ph/

(f) Korea

The personal information protection law in Korea is one of the strictest across the globe[28]. The country currently adopts a sectoral approach in personal information protection, with the Personal Information Protection Commission at the forefront, serving as the top-level data protection authority to supervise personal information processing by the constitutional agencies, central administrative agencies, and local government. The Korea Communications Commission and the Financial Services Commission supervise the data processing activities of the telecommunications sector and financial sector respectively; and the Ministry of the Interior and Safety regulate the rest in the private sector[29].

The sectoral approach seems to cause confusion to individuals and businesses, and a lack of consistency in the application of privacy principles. Therefore, the Korean Government has decided to unify different data protection laws and functions into the Personal Information Protection Act and the Personal Information Protection Commission. The relevant bill has been submitted to the National Assembly. The bill also aims at bringing GDPR elements, such as legitimate interests and pseudonymisation, to the data protection law of Korea[30].

(g) India

In India, nine justices of the Supreme Court of India ruled unanimously in 2017 that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty", and as a part of the freedoms guaranteed under India's Constitution[31]. The lead judgment called for the government to create a data protection regime to protect the privacy of the individual. It

---

[28] Chaeho Rheem, "*How Privacy Culture Has Evolved in Korea over Time*", a paper for the 39th International Conference of Data Protection and Privacy Commissioners held in Hong Kong in September 2017 (page 94):
https://www.privacyconference2017.org/eng/files/programme_booklet.pdf

[29] Hyun Ik Kim, "*About the Personal Information Protection Commission (PIPC), Korea*", ICDPPC Newsletter, Vol.1, Issue 1, 2019 (pages 11-12):
https://icdppc.org/wp-content/uploads/2015/02/ICDPPC-Newsletter-%E2%80%93-Volume-1-edition-1-%E2%80%93-January-2019.pdf

[30] Ditto

[31] *Justice K.S. Puttaswamy (Retd) v Union of India*, Supreme Court of India (Aug 2017): https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

recommended a robust regime which balances individual interests and legitimate concerns of the state.

Following the footsteps of the Supreme Court judgment, the draft Personal Data Protection Bill 2018 was released in July 2018[32]. A number of provisions in the bill mimic the requirement of the GDPR, such as individuals' rights to data portability and data erasure; organisations' obligations to adopt privacy by design, conduct data protection impact assessment and appoint data protection officers in certain situations; and extra-territorial application of the data protection law.

(h) New Zealand

Farther from home but with a similar common law system in New Zealand, the *Privacy Bill 2018* is now before the Parliament, and is intended to repeal and replace the current *Privacy Act 1993*[33]. The Bill retains the existing complaints system, and introduces additional ways to enforce the information privacy principles. Major changes made in the Bill include mandatory reporting of privacy breaches, strengthening cross-border data flow protections, introduction of new offences, and strengthening the Privacy Commissioner's investigative powers.

3.4 Convergence in Regulatory Concepts - Breach Notification; Fines; Extraterritoriality; Data Portability

Developments in data transfer mechanisms such as the EU-Japan mutual arrangement, as well as debates concerning the EU-US Privacy Shield, reveal the steps that might be necessary if trading partners wish to establish a legal regime that is considered adequate to ensure the free flow of data within those jurisdictions.

---

[32] Mayuran Palanisamy and Ravin Nandle, "*Understanding India's draft data protection bill*", IAPP Privacy Tracker, 13 September 2018: https://iapp.org/news/a/understanding-indias-draft-data-protection-bill/

[33] *Privacy Bill 2018*: http://www.legislation.govt.nz/bill/government/2018/0034/latest/whole.html ; *Privacy Act 1993*: http://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html

Secondly, it indicates that even though the standards set by the GDPR may not be legally applicable to other jurisdictions, data protection agencies around the world are marching inexorably towards a gradual convergence in global regulatory concepts, if not regimes.

Regulatory tools such as mandatory data breach notification, data protection authority's power to impose administrative fines, extraterritorial application of data protection laws, and enhanced data subjects' rights (right to erasure and data portability) are either on the wish list of privacy lawmakers, or at least being hotly debated and considered in many jurisdictions.

4. Review of the Hong Kong Personal Data Privacy Law

4.1 PDPO Amendments 2012

The PCPD has a statutory obligation to review the PDPO from time to time to align the regulation with societal and technological development. The last review exercise of the PDPO was conducted in 2009-2012. Totally 56 proposals of amendments were submitted by the PCPD to the Government at that time[34]. The significant change, amongst others, brought by the 2012 amendments of the PDPO was the tightening up of the regulation on direct marketing as a result of a high-profile incident relating to the improper selling of customers' personal data by a customer reward scheme for use in direct marketing. The amendments significantly increased the penalties for misuse (including improper transfer) of personal data for direct marketing purposes to a maximum fine of HK$1,000,000 (US$128,000) and imprisonment for five years. The 2012 amendment also empowered the PCPD to provide legal assistance in meritorious cases to aggrieved data subjects to seek compensation from data users for damage suffered by reason of contravention of the requirements under the Ordinance. A new offence for disclosing personal data obtained without consent from data

[34] PCPD's amendment proposals submitted to the Government during the PDPO Review 2009-2012:
https://www.pcpd.org.hk/english/data_privacy_law/amendments_2012/files/Annex_proposals_to_amend_PCPD_e.pdf

users was also introduced. Other amendments include strengthening the PCPD's enforcement power and imposing indirect regulation on data processors through data users[35].

4.2 Current Review of the PDPO

With the rapid advance in innovation and technology, and in the wake of the global regulatory tsunami dramatically altering the global privacy regulatory landscape, as well as an increasing number of high-profile data breaches over the last few years, it is high time that Hong Kong conducted a review of its data protection law again to strengthen public confidence in personal data protection, and to ensure that Hong Kong is not left behind as a "risky" jurisdiction for hosting data[36].

Over the last two decades, the enforcement focus of data privacy law in Hong Kong, like other jurisdictions, has seen a regulatory shift from collection and use of data to data security. In 2018, the PCPD attended to 129 data breach notifications (a 21.7% increase year-on-year) by way of compliance checks and/or investigations, even though data breach notifications in Hong Kong are not mandatory but voluntary. For all data breach incidents reported, the PCPD spares no time and efforts in engaging the organisations to take immediate remedial actions to contain potential harm to data subjects, and take steps to re-establish their consumers' confidence with a view to minimising consumers' defection. This has been the PCPD's standard initial response to data breach notifications.

Recent high profile data breaches around the world have several significant effects. First, they demonstrate that large, well-resourced global organisations are not immune from major data breaches. Significant or even catastrophic data security or data misuse incidents have caused immense

[35] See Information Leaflet: An Overview of the Major Provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012: https://www.pcpd.org.hk/english/data_privacy_law/amendments_2012/files/ordinance2012_overview_e.pdf

[36] Gabriela Kennedy and Karen H.F. Lee, "*Hong Kong: Change It Up: Amendments To The Hong Kong Personal Data (Privacy) Ordinance Being Considered*", Mondaq.com, 9 January 2019: http://www.mondaq.com/hongkong/x/769550/Data+Protection+Privacy/Change+It+Up+Amendments+To+The+Hong+Kong+Personal+Data+Privacy+Ordinance+Being+Considered

reputational and financial damage to major international airlines; hotel chains; credit reference agencies; and internet forums and service providers.

Second, in the era of digital technology of big data and the Internet of Things, a data security incident frequently involves databases containing a massive amount of personal data. As the variety of data being gathered is wide, so is the impact on the community (data subjects) in the event of a data breach. The number of people affected inevitably involves millions. The potential harm is hard to assess and often may not be immediately apparent – the happening of a data breach may take years to be detected.

Third, significant data security incidents provoke the ire of the general public and focus the attention of lawmakers and law enforcers on the shortcomings of the existing law. It nevertheless exacerbates the impetus for change.

Change has been called for – it is necessary for Hong Kong to have laws that keep up with technology development and international trends. Yet, a balanced approach is paramount. The Chair of the US Federal Trade Commission insightfully warned that if privacy regulation is not formulated cautiously, it "*could have an adverse impact on competition, potentially by entrenching the major digital platforms*" – indicating that large technology companies have resources to spend on compliance, which could give them an edge over mid-size and smaller players if regulation is over-burdensome, and that would be counterproductive[37]. Industry leaders also warned that: "*Every government is itching to regulate, and the risk we all have is that there's a great overreaction. The casualty is the whole digital economy.* [38]"

In considering reform of our personal data privacy law, the PCPD had due regard to all factors and circumstances in balancing the protection of privacy and the free flow of information as well as other freedoms,

[37] Joseph Simons, speech at a US House of Representatives Judiciary Subcommittee hearing on antitrust enforcement, 12 December 2018: https://adexchanger.com/privacy/ftc-chair-simons-supports-federal-privacy-legislation-but-urges-caution/

[38] IBM CEO Ginni Rometty, speech at the World Economic Forum in Davos, Switzerland, 22 January 2019: https://www.cnbc.com/2019/01/22/ibms-rometty-on-privacy-regulations-the-casualty-is-the-digital-economy.html

considering that personal data privacy right is a fundamental human right in Hong Kong guaranteed not only specifically under the PDPO, but also generally under Article 17 of the 1966 United Nations International Covenant on Civil and Political Rights (by which Hong Kong has been abiding since 1976), which is mirror-imaged in Article 14 of the 1991 Hong Kong Bill of Rights Ordinance (Cap 384, Laws of Hong Kong) and constitutionally under Article 39 of the Basic Law of the Hong Kong Special Administrative Region of the PRC. These factors and circumstances also include:

- the legitimate purpose of the reform;
- the pressing need for the reform;
- the proportionality between the proposed change and the pursuance of the legitimate aim;
- the global privacy landscape;
- the local circumstances;
- the interest of all stakeholders; and
- the interest of the community at large.

The scope of the current PDPO review broadly falls into 2 categories: the first category is to identify measures to address the inadequacies of the current voluntary data breach notification regime and other issues which have surfaced as a result of the recent data breaches; the second category is to re-visit issues that have been raised at the last PDPO review exercise in 2009-2012 but were not pursued, as well as to study the new elements brought by the GDPR[39].

Based on the preliminary results of the current review, the PCPD considers that the following issues are, among others, of high priority:

(a) Mandatory breach notification

At present, Hong Kong operates a voluntary data breach notification regime. The PCPD has published the "*Guidance on Data Breach Handling*

[39] See information leaflet "European Union General Protection Regulation 2016", published by the PCPD in March 2018: https://www.pcpd.org.hk/english/data_privacy_law/eu/eu.html

and the Giving of Breach Notifications" (last revision October 2015) to facilitate voluntary breach notification.

The recent massive data leakage incident by a carrier highlighted the inadequacy of a voluntary breach notification regime. Data breach notification is currently at individual data controllers' discretion, as a result of which some data controllers either not give breach notification or give delayed notification. In both scenarios, data subjects' interests would be undermined as the opportune time for data subjects to take action to mitigate the risks and damage of data security incidents could be missed. Legislative changes are called for to plug the loophole, as revealed in public debates. Besides, the global data protection landscape has moved towards a mandatory breach notification regime, backed by sanctions to ensure organisations' compliance.

Under GDPR, organisations are required to notify the data protection authority of a data breach without undue delay (and should not be later than 72 hours, where feasible) after having become aware of the breach, unless it is unlikely to result in a risk to the rights or freedoms of natural persons[40]. Communication to data subjects is triggered "when [it] is likely to result in a high risk to the rights and freedom of natural persons" and such communication should be effected "without undue delay". Unlike the notification to the data protection authority, there is no specific time period for notification to impacted individuals though.

In Australia and Canada, notification is required to be given to the data protection authority and the impacted individuals when there is "a real risk of (or likely to result in) serious harm" or when the breach creates "a real risk of significant harm" to an individual.

It is noted that where the reporting threshold is not high, it may result in over-reporting and thus lead to "notification fatigue" to the impacted individuals and impose onerous administrative burden on both businesses and the regulatory authority. One of the objectives of a mandatory breach notification regime is to protect the interests of the impacted individuals who can take immediate action to mitigate the risk arising from a data

[40] Article 33 of GDPR.

breach incident. Hence, if the risk of harm to the individuals caused by a data breach is not substantial or the risk of harm is not real, notification of such breaches to the data protection authority and the individuals may not serve any practical purpose.

(b) Power to impose administrative sanctions such as monetary penalties

Currently, organisations that contravene the Data Protection Principles under the PDPO will not be liable to monetary penalties until the Enforcement Notices issued by PCPD are not complied with, and as and when the court so determines upon conviction, after criminal investigation and prosecution. It is often described that the offender of even the most serious breach is always given a second chance under the PDPO if the offender complies with the PCPD's directives set out in an Enforcement Notice.

Under GDPR, all EU data protection authorities have power to impose administrative fine for breach of the GDPR provisions. Administrative fines up to €20 million (US$22.6 million) or up to 4% of the total worldwide annual turnover of preceding financial year, whichever is higher, shall be imposed on data controllers / data processors if they fail to comply with provisions under the GDPR. Failure to comply with the mandatory breach notification requirement under the GDPR could attract administrative fine up to €10 million (US$11.3 million) or up to 2% of the total worldwide annual turnover of preceding financial year, whichever is higher. The Singapore data protection authority also has power to direct an organisation to pay a financial penalty of an amount not exceeding SG$1 million (US$735,000)[41] for failure to comply with the requirements under of Parts III to VI (on data collection, use, disclosure, access, correction and care) of the Personal Data Protection Act 2012.

Australia, Canada and New Zealand data protection authorities do not have power to impose administrative fines, although their respective data protection laws provide for or there is already proposal for (e.g. New Zealand) a civil penalty or a fine be imposed by Court for serious and

[41] Section 29(2)(d) of the Personal Data Protection Act 2012.

repeated interferences with privacy. The civil penalty provisions under the Australian Privacy Act allow for a fine of AUS$420,000 (US$330,000) for a serious or repeated interference with privacy, with a maximum penalty of five times of that, or AUS$2.1 million (US$1.65 million).

New Zealand has a draft Privacy Bill 2018 before its Parliament. For mandatory breach notification, it is proposed in the draft Privacy Bill that failure to report will attract a criminal fine of up to NZ$10,000 (US$6,700). New Zealand Privacy Commissioner in his submission on the Privacy Bill 2018 to the government has proposed to replace the NZ$10,000 fine with heavier sanction in the form of an Australian style civil penalty provision, enabling the High Court to impose civil penalty up to NZ$1 million (US$670,000) for organisation and NZ$100,000 (US$67,000) for individuals for serious and repeated breaches.

Under the Canadian regime, the Court also has power to impose up to CA$10,000 (US$7,500) for breach of the mandatory breach notification provisions that came into effect on 1 November 2018.

Effective enforcement can only be achieved if regulatory authorities are provided with appropriate enforcement tools. Administrative fine is generally accepted as an enforcement tool that is more expeditious, informal and cost-effective than the traditional Court-imposed fine for breaches of data protection law provisions.

(c) Direct regulation of data processors

Currently, only data users / controllers are held responsible under the PDPO for violations of the PDPO, but not their data processors. PDPO adopts indirect regulation of data processors requiring data users to supervise data processors by using contractual or other means to ensure processors' compliance with security and retention obligations under the PDPO.

The GDPR effectively adopts a combination of direct and indirect regulation of data processors. It requires data controllers to only appoint or choose data processors that provide sufficient guarantees in respect of technical measures and organisational measures in such a manner that processing will meet the requirements of the GDPR. In this regard, the

GDPR provides specific clauses that must be included in a contract with a data processor. In addition, the GDPR directly regulates data processors by imposing obligations on data processors, such as keeping records on processing activities; cooperating with supervisory authority on request; ensuring security of processing and reporting data breach to the entrusting data controller; restriction to further sub-contract without authorisation from the entrusting data controllers etc.

(d) Data retention period

In this digital era, personal data is increasingly being collected through digital means and stored in cloud, as opposed to being collected and stored in the traditional mode of paper form. Regular data purging is a measure that data users/controllers should undertake to minimize the risk of exposure during a cybersecurity incident.

The current PDPO regime requires that personal data is not kept longer than necessary for the fulfilment of the purpose for which the data is used, and data users/controllers should take practicable steps to erase personal data that is no longer necessary, unless the erasure is prohibited by other laws or it is in the public interest to retain such data (Data Protection Principle 2 and section 26 of the PDPO).

As revealed by recent incidents that involved data that should have been erased, the PCPD takes notice of the calls for fine-tuning the data retention principle and the data erasure obligations to require data users/controllers to formulate and publicize data retention policy, and to make non-compliance with such policy punishable by way of an administrative fine.

5. From Compliance to Accountability to Data Ethics

Globalisation of commercial and data processing activities means that businesses now have to comply with multiple regulatory regimes. Given the uneven data protection landscapes across the globe, due diligence has to be exercised by businesses to ensure that they do not fall short of the legal requirements in the jurisdictions in which they have operation. This mission is proved to be challenging to businesses by a few high-profile data

breaches in recent years in which individuals in multiple jurisdictions were affected, leading to the probes by multiple regulators at the same time.

Meanwhile, despite relentless attempts to revamp data protection laws, the development of technological innovation invariably outpaces regulatory efforts. As a result, meeting regulatory requirements alone would not be effective enough to adequately protect and live up to individuals' expectations in privacy protection, especially in jurisdictions which lack robust deterrent sanctions.

Organisations in general that amass and derive benefits from personal data should be held to a higher ethical standard that meets the stakeholders' expectations alongside the requirements of laws and regulations. Reiteration by enterprises about their compliance with regulatory requirements does not spare them from the devastating damage to their hard-earned corporate reputation and consumers' trust. In this regard, data ethics could bridge the gap between legal requirements and the stakeholders' expectations. It is time for data users/controllers, as well as regulators, to promote and practise data governance and ethics.

Compliance with statutory requirements has sometimes been taken as burdensome, if not a cavalier job or a liability. Since 2014, the PCPD has been advocating a paradigm shift through the Privacy Management Programme (**PMP**) by which the law and good practices could be entrenched, and compliance transforms to accountability alongside the commitment of the top management in corporate governance. Accountability is the mechanism for assuring data stewardship and protection. Data privacy is no longer a legal compliance concern only, but also a business concern which should be addressed by C-suite top management as a corporate governance concern, linking internal policies with data protection law. Businesses ought to treat privacy as an asset rather than a liability – as an opportunity to cultivate a competitive advantage that wins market reputation and the trust of customers.

While the resonance of accountability starts to tune up, the PCPD has been advocating complementing compliance with the law by the adoption of data ethics, which is believed to be the bedrock for nurturing and flourishing personal data protection in times of change.

The PCPD commissioned a study on data ethics in 2018, with a view to drawing up recommendations on what an Ethical Data Stewardship framework should look like, and providing tools for organisations to achieve fair and ethical processing of personal data. The study report[42] was published in October 2018, recommending that organisations who conduct advanced data processing activities should implement ethical data stewardship by adhering to the three core ethical values – **respectful**, **beneficial** and **fair** – and conducting ethical impact assessments, amongst other things. The objective of ethical data stewardship is to ensure that the impact on the interests, rights and freedoms of all stakeholders are duly considered and addressed in data processing activities.

Data ethical values focus on fairness, respect and mutual benefits. In practical terms, they involve genuine choices, meaningful consent, absent of bias or discrimination, and fair value exchange between individuals (data subjects) and organisations (data users/controllers).

At the 40th International Conference of Data Protection and Privacy Commissioner held in Brussels in October 2018, a Declaration on Ethics and Data Protection in Artificial Intelligence was passed, of which the PCPD was one of the co-sponsors. The Declaration sets out six guiding principles to preserve human rights in the development of artificial intelligence, i.e. (i) fair; (ii) continued attention and vigilance; (iii) transparency and intelligibility; (iv) ethics by design; (v) empowerment of every individual; and (vi) reducing and mitigating biases or discriminations. A new permanent working group has been set up pursuant to the Declaration to further promote and develop the six guiding principles across the globe. Being one of the co-chairs of the permanent working group, the PCPD will continue to work closely with multi-stakeholders, both at home and abroad, to nourish a culture and environment that respects privacy. It is hoped that a proper balance would be struck between privacy protection and free flow of information that will facilitate and not hinder technological innovation.

---

[42] See the study report "*Ethical Accountability Framework for Hong Kong, China (2018)*" and "*Data Stewardship Accountability, Data Impact Assessments and Oversight Models - Detailed Support for an Ethical Accountability Framework (2018)*" on the PCPD's website: https://www.pcpd.org.hk/english/resources_centre/publications/surveys/surveys.html

6. Regulating for results

A data protection authority should focus on regulating for results by playing three concurrent roles: first and foremost as an enforcer of the law, second as an educator, and third a facilitator[43].

Effectiveness of law enforcement depends on the efficacy of the law and the enforcement powers of the regulator. A strong data protection regime can resolve concerns about data security and data privacy, clearing the way for the use and sharing of data[44]. In this regard, the PDPO must be kept up-to-date to tackle the new data protection challenges in the data-driven economy.

However, law enforcement alone is not enough to drive compliance and effective protection. A data protection authority should also be an educator to assist organisations in compliance. Meanwhile, too strict the law may slow down innovation and economic development. Hence, a data protection authority should also be a facilitator to strike a proper balance. That is where data ethics and data stewardship come in. Regulators need to work collaboratively with both consumers and businesses, not only to do what they have to, but what they ought to, in terms of being respectful, beneficial and fair in data processing, in order to nourish a culture that respects privacy and data control of individuals, to facilitate businesses and other data users and controllers to further their innovative developments, as well as to evenly distribute the dividends of the digital economy.

7. Unique and Irreplaceable Attributes of Hong Kong within China

There is no dispute that there are a number of factors attributing to the development and success of Hong Kong under the "One Country, Two Systems" principle within the PRC, as was repeatedly acknowledged by the State leaders. Notably, the "free flow of information" and "English as one

[43] Centre Information Policy Leadership, "*Regulating for Results: Strategies and Priorities for Leadership and Engagement*" (25 September 2017)
[44] Herbert Chia, *Five Insights on Data from Academician Wu Hequan*, Hong Kong Economic Journal, 9 January 2019

of the official languages" are two of the "unique and irreplaceable attributes", even though they are seldom stressed in this context. The third one is undoubtedly Hong Kong's protection of personal data privacy right as a fundamental human right, which goes hand in glove with the free flow of information.

Hong Kong is uniquely a common law jurisdiction within the PRC, exercising jurisprudence similar to many of our international trading partners such as the UK and the US. Hong Kong has a legal system that practises and respects international law, particularly in the areas of human rights and international commerce. One of the strengths of Hong Kong within that system is its adherence to the Rule of Law, and a respected and independent judiciary – where justices of the highest court comprise former senior members of the judiciary from other common law jurisdictions.

The fact that the Hong Kong SAR has a privacy culture and legislative protection regime independent of the Government would, amongst others, make the Hong Kong SAR an ideal data hub or centre within the PRC, not least for the Belt and Road, as well as the Greater Bay Area initiatives.

8. Closing

Whilst the PCPD, as the privacy regulator of Hong Kong, will continue to **enforce** the law fairly and **educate** all stakeholders, individual data subjects and organisational data users/controllers alike, and remain vigilant for the privacy concerns about the use of ICT and Big Data as expected of any responsible regulator, the PCPD stands ready and is well poised to **facilitate** the implementation and success of initiatives put forward by both the public and private sectors, as one of the objectives of the PDPO, like others globally, is not to stifle but facilitate legitimate trade, ICT growth and administrative efficiency in the interest of the public.

- End -