

Handout from Stephen Kai-yi Wong, Privacy Commissioner for Personal Data, Hong Kong





香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

**The 11th Annual Sedona Conference
International Programme on Cross-Border Data Transfers
and Data Protection Laws**

The Langham Hotel, Hong Kong

Data Protection Authority (DPA) Roundtable

18 June 2019 (Tuesday)

2:00 p.m. – 3:30 p.m.

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

Introduction

The data protection law of Hong Kong – the Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong Kong (“PDPO”) 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 protection¹. 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 centre².

The OECD Privacy Guidelines 1980 and the EU Data Protection Directive 1995 are widely regarded as the first and the second generations of data protection standards respectively. In April 2016, the EU created the third generation standard by enacting the General Data Protection Regulation (“GDPR”) as a response to technological development, in particular the data technology, in the last two decades³. The GDPR has come into force on 25 May 2018⁴.

In Hong Kong, the use of data technology by both the public and private sectors has become increasingly prevalent. In December 2017, the Government published the “*Hong Kong Smart City Blueprint*” (the “Blueprint”) setting out

¹ The Law Reform Commission of Hong Kong, “*Reform of the Law Relating to the Protection of Personal Data*” (August 1994), paragraph 17.9

² The Law Reform Commission of Hong Kong, “*Reform of the Law Relating to the Protection of Personal Data*” (August 1994), paragraph 5.2

³ Graham Greenleaf, “*2017 Survey of Privacy Law Worldwide*”, Privacy Laws & Business Special Report, February 2017

⁴ See Information Booklet “European Union, General Data Protection Regulation 2016 (Effective 25 May 2018)” issued by PCPD, available at : https://www.pcpd.org.hk/english/resources_centre/publications/files/eugdpr_e.pdf

policy objectives to pursue smart city development by making use of innovation and technology, among others. 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 technology hub and advanced manufacturing centre within the next few years. Adoption of technology like artificial intelligence, blockchain, cloud computing and data analytics is also on the rise in the private sector.

With the rapid adoption of innovation and technology and the change in the global data privacy landscape, it is high time we conducted a review of the data protection law in Hong Kong to strengthen confidence in personal data protection and ensure that Hong Kong is not a “risky” jurisdiction for hosting data⁵. These are crucial factors to maintain and improve Hong Kong’s competitiveness in the data-driven economy. This paper seeks to explain how the free flow of information and personal data protection regime have been working as one of the “unique and irreplaceable attributes” of the Hong Kong SAR within one country; discuss some of the possible reforms of the data protection regime in the midst of the global evolutionary privacy landscape; outline how data governance and ethics would complement data law enforcement; and the ways our data protection framework could facilitate Government’s policy pursuing Hong Kong as a smart city.

1. Privacy Legal Framework

Privacy right is a fundamental human right in Hong Kong protected comprehensively under the PDPO; as stipulated in Article 17 of the 1966 United Nations International Covenant on Civil and Political Rights which is mirror-imaged in Article 14 of the 1991 Hong Kong Bill of Rights Ordinance (Cap. 383, Laws of Hong Kong) and guaranteed as it applies to Hong Kong under

⁵ 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

Article 39 of the Basic Law of the Hong Kong SAR of the PRC. The PDPO was drafted and enacted with reference to, if not modelled on, the OECD Privacy Guidelines 1980 and the EC Data Protection Directive 1995. This fundamental privacy right is accepted as a pre-condition for enjoyment of and the basis for many other different rights, including the freedom of expression and free flow of information. Inevitably, there are instances where these rights may conflict with one another. Regulators are duty bound to strike the proper balance.

Unique and Irreplaceable Attributes

There is no dispute that there are a number of factors attributing to the development and success of the Hong Kong SAR under the “One Country, Two Systems” principle within the PRC, as also acknowledged by the State leaders. Notably, the “free flow of information” and “English as one of the official languages” are two of the “unique and irreplaceable attributes”⁶, albeit seldom stressed in this context.

Like many other jurisdictions, the Hong Kong PDPO provides for protection during the entire life cycle of data that identifies a person (data subject) against unlawful, unfair, excessive and obscure collection, unwarranted retention, unauthorised use and disclosure; insecure storage and accidental loss; failure to give a comprehensible policy statement and wrongful handling of requests to access data on the part of those who control and process the data (data users), individuals and organisations (private or public and the Government) included⁷.

Casting in letters on our statute book a single set of comprehensive personal data principles, with sanctions, certainly helps, alongside other statutory

⁶ See Xi Jinping, Speech at the meeting with Hong Kong delegation in the Celebration of the 40th Anniversary of the Reform and Opening Up of the Country (12 November 2018); Zhang Dejiang, Keynote Speech at the Belt and Road Summit held in Hong Kong (18 May 2016)

⁷ See Schedule 1 to the PDPO, the 6 Data Protection Principles

protections, reinforce the certainty of enjoying the free flow of personal information which has been one of the core values of freedoms in Hong Kong.

Similar set of legal regimes protecting personal data does not appear to exist in the mainland of China, although the similar spirit of the law can be found in isolated and subject-specific policies, legislation and regulations⁸. That said, the mainland authorities are catching up fast and working hard putting in place data protection measures. More recently, the Cybersecurity Law 2017, which regulates the processing of personal information by network operators, came into force on 1 June 2017. It strengthens data protection regime in the mainland of China. The General Provisions of the Civil Law (the “General Provisions”), which came into effect on 1 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/her privacy or personal information right is infringed. In December 2018, the State Council of the mainland China 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 respect and protect human rights enshrined in the Constitution, which includes the rights to personal dignity and privacy of correspondence. 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. This means that the conditions for legislation are mature and the relevant bill will be deliberated by the Standing Committee within its current term.

The magnitude of personal data, online in particular, collected, retained, used and stored in a massive country like the mainland of China needs no deliberation or illustration. Mainland China's contribution to the evolution of

⁸ See Cybersecurity Law; E-Commerce Law; Law on the Protection of Consumer Rights and Interests; Criminal Law; General Provisions of the Civil Law; Personal Information Security Specification; and Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information, etc

data-driven economy and the related digital ecosystems, FinTech and Artificial Intelligence in particular, coupled with the phenomenal change of the global data privacy landscape, the extra-territorial jurisdiction in enforcement in particular, has arguably flagged up the urgent need for a data protection framework that would meet the international standard and the aspirational expectation of its data subjects.

At the 39th International Conference of Data Protection and Privacy Commissioners held in Hong Kong in 2017, the sharing and discussion about privacy cultures of the West and the East revealed that in some “Eastern” jurisdictions the concept of privacy virtually had not existed in their traditional culture owing to their conventional philosophy, political and social development. But the demand for personal data privacy protection was picking up its momentum after having gone through economic reforms whereby awareness and expectation of their people gradually gathered force. Scholars argued that on top of cybersecurity, attention was turned to controlling what data was flowing in and out of the jurisdictions. Instead of a fundamental human right of a person, data privacy right is taken as a community right, or national interest, and data is a sovereign asset rather than an individual’s. For many other multinationals in the world, the different privacy culture may understandably be a source of worry.

Different Privacy Culture; Comprehensive Data Protection Regime – Ideal Data Hub within the Country

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 mainland of China, not least for the Belt and Road, as well as the Greater Bay Area initiatives.

Transfer of Data

The conditions under which an organisation may transfer personal data out of a jurisdiction vary from legislation to legislation. Broadly speaking, four common legal bases are adopted worldwide:

- (a) White List (of countries/jurisdictions);
- (b) Certifications (of organisations);
- (c) Safeguards (by law); and
- (d) Consent (by individual data subjects).

In Hong Kong, similar conditions (except (b)) are set out in section 33 of the PDPO. Despite the fact that the provision is yet to come into force (very much due to the feedback and concerns of the business sector especially the SMEs on the impact and implementation difficulties that section 33 would have on them), for any cross-jurisdiction transfer of data, a data user is required to give notice to the data subject of the classes of the transferees of the personal data pursuant to Data Protection Principle 1(3) under the PDPO.

To provide practical guidance for data users to prepare for the implementation of section 33 of the PDPO, the office of the Privacy Commissioner for Personal Data, Hong Kong (“PCPD”), which is statutory authority independent of the government, published “Guidance on Personal Data Protection in Cross-border Data Transfer”⁹ in December 2014. Data users are encouraged to adopt the practices recommended in the Guidance as part of their corporate governance responsibility. The Guidance provides for various ways to effect cross-jurisdiction data transfer. For example, data transfer can be effected through data transfer agreements with overseas recipients, incorporating the model

⁹ See Guidance Note on Personal Data Protection in Cross-border Data Transfer published by PCPD in December 2014 and available at:

https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf

clauses as recommended in the Guidance, which is de facto one of the models adopted by a great number of jurisdictions worldwide. Another way that data users can effect data transfer is based on consent of the data subjects.

In 2016, the Hong Kong SAR Government commissioned a consultant to conduct a Business Impact Assessment (BIA) Study on the issue of cross-border/boundary data transfer. In late 2018, the PCPD commissioned another consultant to explore how restrictions on cross-border/boundary data transfer may be implemented in the wake of the issues or concerns identified by the BIA study. It is expected that a report will be ready by the end of the first quarter of 2019.

2. Data Breaches

Over the last two decades, Hong Kong, like other jurisdictions, the enforcement focus of data privacy law has seen a regulatory shift from collection and use of data to data security.

Last year (2018), we attended to 129 data breach notifications (a 21.7% increase year-on-year) by way of compliance checks and/or investigations, despite the fact that data breach notifications in Hong Kong are not mandatory but entirely voluntary. Whether it should remain voluntary is of course a matter for review especially after a number of major data breach incidents involving millions of data subjects. As in the case of travel agents having been cyber-attacked and data hacked, the PCPD spares no time in engaging the enterprises/organisations to take immediate remedial actions to contain the possible damage to customers/data subjects, and take steps to re-establish their consumers' confidence and reduce consumers' defection. This has been our standard initial response to data breach notifications.

3. Incentivising and Engaging

It remains our primary duty to fairly enforce the data protection law and we spare no sticks in this respect. We do not, however, aim to bump up investigation or prosecution figures. We do seek to address the root of the complaints, grievances and data breaches by engaging the parties concerned with a view to coming up with remedial actions in good time, and preventing similar incidents from recurring. Deterrent sanctions, however heavy, may not always have pronounced effect on future behaviour violating the law; worse still where the sanctions are not deterrent enough. Whilst carrying a big stick, we also provide guidelines, practical assistance (including data audit process like Privacy Management Programme) and support for compliance and good practices. The carrots should also take the form of positive, open and constructive engagement. Engaging the stakeholders, businesses and private organisations in particular, to “get it right” tops our priorities, through incentivising, education, training, publicity, consultation, frank exchange and providing support for regulatory sandboxes. The response and feedback have, so far, been most encouraging.

4. Data Governance and Data Ethics

Compliance with the statutory requirements has sometimes been taken as burdensome, if not a cavalier job or a liability. Since 2014, we have 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 CEOs in the boardroom rather than in the back room, linking internal policies to data protection law, adopting the Privacy by Design

approach by bringing privacy to the foreground and embedding privacy from the outset. Businesses should treat privacy as an asset rather than a liability; a competitive edge that wins market reputation and trust of customers. It is of paramount importance that organisations, SMEs in particular, should be engaged. Our efforts in this respect have been intensified over the last few years.

While the resonance of accountability starts to tune up, we have been advocating complementing compliance with the law by the adoption of data ethics, which we believe are the bedrock for nurturing and flourishing personal data protection in times of change.

Data ethical values typically centre at fairness, respect and mutual benefits. In practical terms, they involve genuine choices, meaningful consent, no bias or discrimination and fair exchange on a level playing field between individuals (data subjects) and organisations (data users/controllers).

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 the data privacy frameworks around the globe which are largely notification or consent-based. Individuals may not even be aware that their personal data has been collected or shared, not to mention exercising control over their data and objecting to unfair or discriminatory use of it, despite the fact that personal data does not belong to any organisation, but the individuals from whom the data is collected.

It is against this background that in April 2018 we commissioned a consultancy study, with a view to drawing up recommendations on what an Ethical Data Stewardship framework should look like, and tools for organisations to achieve fair and ethical processing of personal data. The consultancy report was published in October 2018. A multi-stakeholder approach is recommended in

the consultancy report. In other words, an organisation has to take into account the rights, interests and freedoms of all stakeholders in planning and conducting its data processing activities. The stakeholders do not only include the clients and customers of the organisation, but also other individuals that may be impacted by the data processing activities, as well as society as a whole. The consultancy report suggests three core values of data ethics, i.e. respectful, beneficial and fair:-

- “Respectful” means an organisation has to show respect to individuals by being transparent in its privacy policies and practice, and allow individuals to exercise control over the processing of their personal data.
- “Beneficial” means that an organisation has to identify and assess the benefits and risks of its data processing activities, and take actions to mitigate the risks.
- “Fair” means that an organisation has to avoid bias, discrimination and other inappropriate actions in its data processing activities.

The full consultancy report, together with an assessment framework and oversight model, can be downloaded from the PCPD’s website www.pcpd.org.hk.

5. Regulating for Results

A data protection authority should regulate for results by playing three roles at the same time: first and foremost as an enforcer of the law, second as an educator, and third a facilitator¹⁰.

¹⁰ Centre Information Policy Leadership, “*Regulating for Results: Strategies and Priorities for Leadership and Engagement*” (25 September 2017)

Effectiveness of law enforcement depends on the efficacy of the law and the enforcement powers of the regulator. A strong data protection can resolve concerns on data security and data privacy, clearing the way for use and sharing of data¹¹. In this regard, the PDPO must be kept up-to-date to tackle the new data protection challenges in the data economy.

However, law enforcement alone is not enough to drive compliance and effective protection. Therefore 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. With data ethics and data stewardship, we will work hand in hand 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/controllers to further their innovation developments, as well as to evenly distribute the dividends of the data economy.

6. Unlocking and Sharing Data Legitimately – Hong Kong as a Smart City

It being our own data, we as individuals are entitled to have the legitimate control, or self-determination, over it – “Personal Data in Our Hands” as we put it. This is principally what is enshrined in our PDPO and re-confirmed by the GDPR. On the other hand, in this data-driven economy that keeps growing in parallel with the big data and ICT developments from which we benefit tremendously particularly in relation to scientific advancement, economic growth and social interactions, it would not be in the interest of the community

¹¹ Herbert Chia, *Five Insights on Data from Academician Wu Hequan*, Hong Kong Economic Journal, 9 January 2019

at large to have data locked up. One of the challenges that we as regulator have to meet in this Age of Artificial Intelligence and Big Data, where sensory ability, cognition, robotics, machine learning etc. enabled by Cloud coming in aid, would probably be how we could 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, identifying and securing the innovative use of personal data in this data-driven economy.

Hong Kong is set to transform into a smart city and Government initiatives have been rolled out. It was announced on 3 January 2019, that Government bureaux and departments, would be releasing 650 new data sets this year, taking the total number of open data sets available to about 4,000 by the end of this year, which is in line with the Chief Executive's Policy Address 2017.

Whilst we will remain vigilant for the privacy concerns about the use of information and communication technology ICT and Big Data in these initiatives as expected of any responsible regulator, we stand ready and we are well poised to facilitate the implementation and success of the initiatives, as one of the objectives of our data protection law, like others globally, is not to stifle but facilitate legitimate trade, ICT growth and administrative efficiency in the interest of the public.