39th International Conference of Data Protection and Privacy Commissioners (ICDPPC)
Opening Ceremony of the Open Session
28 September 2017
Kowloon Shangri-La, Hong Kong

Speech by
Stephen Kai-yi Wong,
Privacy Commissioner for Personal Data, Hong Kong

Secretary for Justice, Mr Rimsky Yuen, GBM, SC, JP;
Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, JP;
Chairman of the ICDPPC, Mr John Edwards;
Distinguished Representatives of the Data Protection Authorities, global and local enterprises;
Ladies and Gentlemen,

Welcome to the Conference, which we in Hong Kong have been waiting for 18 years to re-host.

For those who have come from places outside Hong Kong, welcome to the vibrant and dynamic city of Hong Kong in China.

I must apologise to those who have to resort to the annex of this hall this morning as we failed to resist the temptation to accommodate those who registered as participants out of time.

Today, we have the largest single mass of global data protection authorities and data related conglomerates under one roof in Asia in history, totalling more than 750 delegates, about 65% of whom coming from 67 countries or territories, with about 80 DPAs and related bodies, as well as 165 data related business enterprises. Special mention must go to the representatives from the 11 countries in Africa, 15 countries and territories in Asia, and 20 delegates from the mainland of China. For our friends in Mexico, we offer our deepest sympathy to those who suffer from the recent natural disasters and most grateful that some have made an effort to come to Hong Kong. For the others, we fully understand why they cannot join us today. You may be interested in the local representation at this Conference in that a great many officers from the public sector of Hong Kong, such as the Department of Justice, the Hospital Authority, the Hong Kong Monetary Authority, the Consumer Council, and the Mandatory Provident Fund Schemes Authority, as well as a large pool of professionals are also joining us.

I must be stating the obvious that today we are living in data driven and digital economies. Data related issues are what we are seeking to discuss today and tomorrow. I am most encouraged to see many of the participants here today come from the emerging economies, which account for half of the global trade flows. Joseph Cannatici (UN Special Rapporteur on the Right to Privacy) once said our mobile phones know more about us than we could imagine. He even went on to say that mobile phone is the informative device that would tell whether one has extra-marital affairs. As Brad Smith (of Microsoft) rightly put it, data is the core and heart of economic development and we are entering the dawn of a new (or the 4th) industrial revolution.

Indeed, we in Hong Kong and China have had a data evolution, if not a data revolution. Our Secretary for Justice has just told you how our data protection laws evolved over the last 20 years. Let me tell you how our daily lives have changed in the midst of this evolution.

For those coming from overseas, you might have heard of the incredible property prices in Hong Kong. To give you some idea, a parking space in a residential block today may easily cost you more than 400,000 Euros – that is a space of a small size car. Above this parking space sits an apartment, amongst perhaps 300 others in the same block, that would cost you 25,000 Euros per square metre, or 2.5 million Euros for an apartment similar to a 2-bedroom flat in London.

About 20 years ago, lots would be drawn for the purchase of residential apartments in Hong Kong. To inform the lucky ones, the results of lottery would be announced by publishing the potential buyers' identity card number in full. These numbers in those days were the most important personal data of the people of Hong Kong. Today, only part of the identity card number is shown.

Out of its population of 7.4 million, Hong Kong has 14.5 million mobile SIM cards in active use, of which 7.5 million with 4G services[1]. When you are inside railway stations here in Hong Kong, you will always hear the announcement urging people not to look at their mobile phones when using the escalators.

If you think that Hong Kong is smart enough, wait till you go to the mainland of China, which starts just 30 kms from where you are now.

The penetration of ICT in the mainland of China is even more intense. On the Singles Day (光棍節) last year, i.e. 11 November, Alibaba's online shopping platform, Taobao, recorded RMB 10 billion transactions within the first 7 minutes of the day[2]. Total transaction value of that day exceeded RMB 100 billion[3]. Who will be more analytical and authoritative than Jack Ma (of Alibaba) when he said we are moving from the era of IT to the era of DT?

A number of mainland cities plan to turn themselves into cashless, in which many of the brick-and-mortar stores will only accept electronic payments[4].

You may wonder what people are doing with the QR codes in the mainland of China.

Not only can shopping in the mainland be cashless, making a donation to the beggars there calls for Fintech, too.

By using these devices, you will inevitably leave your digital footprints. Extensive use of ICT has led to the creation of location data or metadata in a massive scale and at an unprecedented speed.

Data breach notifications received by the Compliance Division of my office has been increasing lately. According to the research by Gemalto, the number of data records lost or stolen in 2013 was 575 million[5]. In 2016, the number further increased to nearly 1.4 billion[6]. Inadequacy in cybersecurity poses imminent and grave threat to privacy.

Extensive collection of personal data, in conjunction with sophisticated data mining and profiling techniques, may expose your innermost secrets, or intimate space, and the results of the analytics can often be biased or embarrassing, often without your knowing it.

Collection and use of personal data are becoming part and parcel of our daily lives. From the day we were born, we have had our data collected and used or processed.

Some of you may have heard of the story of how voters were nudged in isolated referendum and election activities by way of data mining and profiling.

Recently in Hong Kong, we had a case where data was collected and used in activities relating to the election of Hong Kong's Chief Executive. One month prior to the election in February this year, a pressure group organised what they called a "civil referendum" activity in which any Hong Kong

---

[1] "Key Statistics for Telecommunications in Hong Kong, July 2017", OFCA:
http://www.ofca.gov.hk/filemanager/ofca/en/content_108/wireless_en.pdf
(Total number of activated SIM cards = Post-paid SIM + Activated Pre-paid SIM)
[2] http://news.qq.com/a/20161111/001946.htm
[3] http://www.bbc.com/zhongwen/trad/china/2016/11/161111_alibaba_singles_day_e-shopping_2016
[4] http://news.xinhuanet.com/fortune/2017-07/06/c_129648891.htm
[5] http://breachlevelindex.com/assets/breach-level-index-infographic2013.jpg
[6] http://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2016-Gemalto-1500.jpg

citizens aged 18 or above could cast their votes for or against certain candidates through a voting system. This voting system adopted an instant communication application for the voting process, which collected participants' identity card number, mobile phone number etc. However, there was no explanation on the purpose and lawful basis for the data collection, the true identity of the data controller was not made known or confusing, and the security of the data collected was dodgy. After a compliance check initiated by me, I urged the pressure group to suspend the activities until remedial actions were taken, and in fact they were subsequently taken, on the basis of unfair collection of personal data and a breach of data security. I will issue revised guidelines in relation to election activities involving personal data and digital identity management.

Changing Global Privacy Landscape

Indeed, the global privacy landscape has changed phenomenally since the implementation of the 1980 OECD Guidelines and the EU Data Protection Directive 1995 which shaped many data protection regimes, including the one in Hong Kong. For example, much of the personal data nowadays (often in an unstructured form) is not collected directly from individuals, but is generated, or derived from their uses of, or interaction with ICT and IoT devices. According to the World Bank, some governments, e.g. Korea, China, Singapore, India and the UK are supporting the development of IoT business incubators and innovation centres, which included platforms and testbeds for startups and SMEs. Africans countries provide the most effective and innovative solution to IoT. The key challenge is how to apply the core principles in data privacy protection which value individual's autonomy and control over his personal data when facing the reality.

It is therefore all the more important for us to keep abreast of the changing privacy landscape worldwide. We all know that the European Union (EU) is undergoing a major reform of their data privacy law. The EU's General Data Protection Regulation (GDPR), which will come into effect in May next year, has introduced enhanced rights to protect individuals' data privacy through "legal and pragmatic approaches" , as Giovanni Buttarelli (European Data Protection Supervisor) described it, providing " a new and unique model for DPAs" as Isabelle Falque-Pierrotin (of the French Data Protection Commission) explained. It is quite clear that the scope of data protection has been broadened by reinforcing current rights and creating new rights.

Against this background, my office has carried out a comparative study between the GDPR and our law. Twelve major differences were identified in our study. Some of these key aspects echoed with key topics to be discussed in this Conference. I would like to share with you some of my initial observations.

Notice and consent

We all know that "notice and consent" is a fundamental legal basis for personal data processing in many jurisdictions. Also, the prevalence of ICT has desensitised us regarding the control over our personal data. Many of us do not bother to read the lengthy privacy policy and tick 'agree' and "accept" boxes without second thoughts. To be fair, do we have a real choice?

The GDPR has further tightened up the criteria for valid consent, requiring the data subjects to explicitly signify their agreement by either "*a statement or a clear affirmative action*" in order to constitute valid consent. And it will be easier for a data subject to withdraw consent.

Though the notion of consent is manifested in our Personal Data (Privacy) Ordinance, our data collection principle (as drafted) emphasises on requiring data users to inform a data subject about the purpose of collection[7]. It also provides that personal data should only be collected for "*a lawful purpose directly related to a function or activity*" of the data user[8]. When a data user wishes to use

[7] Data Protection Principle 1(3) of the Personal Data (Privacy) Ordinance: "*Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that…he is explicitly informed…the purpose… for which the data is to be used…*"

[8] Data Protection Principle 1(1) of the Personal Data (Privacy) Ordinance

the data for a different purpose, it has to obtain the *"prescribed consent"* from the data subject, which is defined as "*express consent of the person given voluntarily"*. It is our regulatory stance that such consent must be *"informed"* and should not be inferred from *"silence and non-response"*. We also treat *"bundled"* consent with reservation.

As regulator, I often ask myself the question: how should we strike a proper balance? Would precise and concise notice suffice? Given the notion of notice and consent has been incorporated under our law, we envisage that there is no pressing need to change our law. That said, we are mindful that data subjects should be given realistic and informed choices; so that there will not be surprises. Hence, elaboration and more guidance on the meaning and scope of consent would be appropriate. Later on today, we are going to put our heads together on this topic of "notice and consent".

Accountability

Data processing by the new technologies is highly automatic, such as machine learning, artificial intelligence, big data analytics and the Internet of Things. It becomes more challenging to ensure transparency and data use limitation.

Accountability and governance may well be a way out for data protection in the ICT age. It motivates organisations to shift from compliance to accountability. The accountability principle was incorporated in the 1980 OECD Guidelines and was retained in its revised 2013 version. Similar requirement will be imposed explicitly on the data controllers in the EU after the GDPR comes into effect.

In Hong Kong, although the accountability principle is not expressed in our law, my office has launched the Privacy Management Programme to encourage organisations to adopt a paradigm shift from compliance to accountability. Explicitly incorporating the accountability principle and certification regime in our law are worthy of further exploring. The PMP is now being fine-tuned through pilot tests in selected public authorities. Certainly we will have due reference to the relevant provisions in the GDPR.

Sanction

The EU's GDPR has set a good example for the legal framework of penalising breaches[9]. An administrative fine up to 20 million Euros, or 4% of the total worldwide annual turnover of preceding financial year, whichever is higher, shall be imposed for serious breaches of the GDPR. As compared with the relatively modest enforcement power we have here in Hong Kong (that is serving enforcement notices to direct organisations to take remedial measures in most of the cases), there is much room to bridge the gap if a robust regime is preferred. This is an area that we as regulator in Hong Kong would like to revisit with a view to taking the case further.

Extra-territorial application

Privacy or personal data protection is becoming a universal value. Today we have around 120 data protection laws enacted globally, and about 30 bills are in the pipeline[10]. The GDPR has explicitly strengthened its scope to non-EU organisations so long as the processing activities are targeting the EU data subjects[11]. In the midst of this digital age, cross-border data flows are surging and connecting more countries. When personal data privacy protection becomes borderless, interoperability of data protection laws and cooperation of data protection authorities are crucial. Given the volume of trade between EU and Hong Kong, we are duty bound to walk the business sector in Hong Kong through the relevant provisions.

---

[9] Articles 83-84 of GDPR

[10] "*Privacy Law & Business – International Report – Special Report*", February 2017

[11] Article 3 of GDPR: so long as the processing activities are related to *"the offering of goods or service to data subjects in the EU or the monitoring of the behaviour of data subjects in the EU"*

My office will publish guidance and organise seminars to help organisations understand the GDPR's standards. We will also discuss the issues and challenges relating to compliance with GDPR with our colleagues at the APEC Forum. At the same time, international cooperation between data protection authorities becomes one of the top priorities despite the variations in our laws. International cooperation should not be limited to enforcement, but also promotion and facilitation of compliance. Through this Conference, we hope we can nurture understanding, cultivate interoperability and cooperation between different regions of the world, in terms of both privacy regulations and privacy culture.

On a separate but related note, the Central Government of China announced its Belt and Road initiative in 2015 to build international trade links by land and sea from East Asia all the way to Western Europe. The routes cover more than 60 countries in Asia, Middle East and Europe[12]. Inevitably, we envisage cross border or cross boundary flow of personal data originating from jurisdictions with different cultural backgrounds and regulatory regimes. Hence, international cooperation between Hong Kong and all the jurisdictions concerned will be critical to assure the security and privacy protection of personal data.

Given the irreplaceable attribute of Hong Kong in respect of the free flow of information, which finds its enabling environment on the protection of freedoms and human rights as guaranteed under the Basic Law, including the working implementation of our data protection law and framework, we are well poised to help make Hong Kong the Belt and Road Data Centre within one country but outside the jurisdiction of the mainland of China, if not a global Data Hub. Tomorrow, you will hear how Hong Kong can facilitate cross-border or cross-boundary data flows and drive digital economy to grow in a healthy way.

From Structure to Culture and Ethics – West and East

The theme of this Conference is "***Connecting West with East in Protecting and Respecting Data Privacy***". You will have views expressed and shared during the course of these two days. Many thanks to the most inspirational report on "Privacy Bridges Programme", which aimed to bridge the gaps between the EU and US data privacy approaches, published by Jacob Kohnstamm (the then Chairman of the Dutch Data Protection Authority) at the 37th Conference held in Amsterdam. You will surely get to know more about the different legal infrastructures and the ecosystems in the West and the East relating to data protection, from their structure to their culture.

The latest Whitepaper released by Google entitled "Smarter Digital City" is most telling. One of the research findings reveals that consumers expect more than selling brand relationship – they request security and trust. Given that data is a sustainable resource, we need to have trust as succinctly put by Liz MacPherson (of Statistics New Zealand). One of our common values is without a doubt the interoperability and interconnectivity to ensure that personal data privacy is not only duly protected but also duly respected. This requires the engagement of all parties – individuals (the data subjects), organisations (the data users, controllers or processors) and the regulators. Between the individuals and organisations, we must get it right. As Stephen Deadman (of Facebook) pointed out, building transparency and control is at the heart of getting it right. If we get it right, organisations will enjoy the fruit of leveraging mutual confidence, trust and respect, thereby meeting the expectation of the individuals. Furthermore, meeting the legal requirements of compliance and accountability to recognise the intrinsic values of data privacy rights would be improved by the ethical approach including a fair and ethical use or processing of data. Data users need to add value beyond just complying with the regulations. Discussions about "New Digital Ethics", the relevant ethical standard and stewardship have already begun. Surely the deliberations will go on. In the not far away future, we may come up with an "Equitable Privacy Right" for all stakeholders.

[12] https://beltandroad.hktdc.com/en/belt-and-road-basics

Ladies and Gentlemen, it is a distinct privilege for us in Hong Kong to be able to provide a meeting place to pick your brains. This Conference brings together so many different interests, all stakeholders and ample opportunities to develop new means of communications and collaborations. Tribute must be paid to the ICDPPC's well established public-private partnership, joined by the academia and research institues as well as our sponsors and supporting organisations, the Governement of Hong Kong Special Administrative Region in particular.

We also aim to ensure that meetings and side events aside, you will thoroughly enjoy your stay in Hong Kong. I did not mention shopping in our bid to host this Conference, I am sure you won't miss enjoying it.

I wish you all a very fruitful Conference and memorable stay in Hong Kong.

Thank you very much indeed.