Hong Kong Commissioner Wong: Upcoming EU and Chinese Privacy Laws Will Get the Limelight

The interview tour around the world continues, giving us a taste of the diversity and importance of the issues which will be discussed at the upcoming 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC). Next stop on our tour: Hong Kong.

We speak with Mr Stephen Wong, the Privacy Commissioner for Personal Data and Co-chair of the ICDPPC Working Group on Ethics and Data Protection in Artificial Intelligence. Commissioner Wong believes Hong Kong privacy laws are due an update to keep up with technological trends and to avoid the jurisdiction getting labelled as risky. Hong Kong's privacy chief expects that the EU ePrivacy Regulation and the new mainland China privacy laws will have a major impact internationally. He echoes the call of his European and Australian colleagues, EDPB Chair Jelinek and Commissioner Falk, for more global convergence to avoid fragmented regional privacy frameworks, and adds the attention to ethics from last year's ICDPPC should be continued. Nelly Stratieva, editor of the European Data Protection Law Review (EDPL), conducts the interview with Commissioner Stephen Wong.

NS: Commissioner Wong, could you tell our readers more about the current privacy and data protection issues and initiatives in Hong Kong?

SW: 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 the 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, the Personal Data (Privacy) Ordinance (PDPO). We want 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.

It is necessary for Hong Kong to have laws that keep up with technological development and international trends. In

considering a reform of our personal data privacy law, the Office of the Privacy Commissioner for Personal Data (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. We keep in consideration that the 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), mirrored 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 People's Republic of China.

Regarding the scope of the current PDPO review, the PCPD considers that the following issues are, among others, of high priority: (a) mandatory breach notification, (b) the power to impose administrative sanctions such as monetary penalties, (c) direct regulation of data processors, and (d) the data retention period.

NS: You hosted the 39th ICDPPC in Hong Kong in 2017 where it seemed that the word in everyone's mouth was the GDPR. What do you think will be the next law that could have a similar disruptive impact internationally? Do you expect it to come again from Europe or from another part of the world?

SW: I believe that when the e-privacy legislation in the EU and the various pieces of legislation on privacy protection in mainland China becoming mature they would be the next in the limelight.

Now that the online world occupies a significant part in our daily lives, what we have in the physical world is increasingly expected to be available in the online world. We have long established laws on various aspects of privacy for the physical world. Likewise, e-privacy is increasingly expected. The GDPR deals with this aspect but only partially. The ePrivacy Regulation intends to regulate not only traditional telecommunications operators, but also 'Over-the-Top' communication services (eg, email, instant messaging such as WhatsApp) to ensure that end-users' confidentiality of communications is protected. The data under protection is not limited to personal data, but also metadata and machine-to-machine communications. The e-privacy legislation will make protection of individuals online more comprehensive.

The mainland of China is catching up in privacy legislation, and is catching up fast, though it does not have one single piece of omnibus legislation covering data protection. The related legislation work is now on the priority list of the National People's Congress. We believe that the effect of the legislation will be far-reaching given the economic status of China in the globe and the high volume of trade between China and other countries.

In the mainland of China, the Cybersecurity Law imposes, amongst others, a data localisation requirement. Under this requirement, operators of critical information infrastructure (such as public communications and information services, energy and transportation) are restricted from transferring personal information and important data to a place outside the boundary of mainland China.

According to a report by the Wall Street Journal in July 2019, the US and many foreign businesses consider those new draft rules and standards as draconian measures for implementing the Cybersecurity Law and represent additional barriers to the Mainland market. Some foreign businesses think these rules and standards forbid certain data from leaving mainland China or at least slow the process of dispatching data, which would increase uncertainties and costs for business. These are the concerns expressed by the relevant stakeholders.

In the face of these concerns and uncertainties, commitment in the form of pledging and certification under certain robust data governance principles developed by trade practitioners and facilitated by regulators can serve as an alternative means to promote trusted data transfers from the mainland of China.

NS: What major issues do you hope will be addressed at the 41st ICDPPC in Tirana? Which topics are of most importance for you?

SW: As technology becomes increasingly pervasive in our lives, no doubt ethics will become even more important. One of the challenges that regulators have to continue to meet will be how they could help unlock and share personal data within the legal and ethical frameworks in the midst of widely applied sensory ability, cognition, robotics, machine learning, cloud services, etc. We can see that complementing compliance with the law by adopting data ethics will form the bedrock for nurturing and flourishing data protection in times of change.

Ethics and data protection was one of the major items at the 40th ICDPPC in Brussels last year, and we foresee that it would continue to be one in Tirana. The PCPD has advocated data ethics for some time. Now it is high time we pushed forward 'ethics by design'. As the co-chair of the ICDPPC Working Group on Ethics and Data Protection in Artificial Intelligence, we would continue to contribute via this platform.

Besides data ethics, we believe that international cooperation on enforcement, in particular the possible tools and mechanism to facilitate, would be another key initiative on the global data privacy arena. Given the global nature of data breaches, every data protection authority affected would have to conduct its own investigation, leading to a waste of resources and possibly divergent results. Meanwhile, fragmented regulatory frameworks around the world, in Asia in particular, have been a major concern for organisations having international or interregional operations. There is hence a pressing need for regulators to work together to bring about fair enforcement outcomes, especially in relation to cases involving multinational organisations. In fact there is no justification for regulators not to put their heads together for a de-fragmented regulatory framework, if not a harmonised one. We should explore the possibilities for collaboration among regulators across jurisdictions in the form of an international agreement to deal with cross-border data breaches effectively. It also echoes the theme of the 41st ICDPPC: Convergence and Connectivity.