ashurst

Latest developments in APAC data privacy

FT INNOVATIVE LAWYERS ASIA-PACIFIC 2022 WINNER

22 JUNE 2022

Agenda

1. Introduction
2. Data privacy update: Hong Kong
3. Data privacy update: China
4. Data privacy update: Australia
5. Data privacy update: Singapore
6. Panel discussion: The future of data privacy in APAC

ashurst

ashurst

Data privacy update: Hong Kong

HOI TAK LEUNG
Counsel, Hong Kong

Background to the PDPO Amendment Bill 2021

On 29 September 2021, the Legislative Council of Hong Kong passed the Personal Data (Privacy) (Amendment) Bill 2021.

"Since 2019, doxxers have attacked those of different political stances through the indiscriminate disclosure of their personal data, in effect weaponising the personal data concerned. The Ordinance aims to combat malicious doxxing acts that have become more rampant in recent years, so as to protect the personal data privacy of the general public. We have to spare no efforts to combat such despicable doxxing acts that have a clear intent to harm, so as to eliminate conflicts in the society and establish the virtues of law-abidance and mutual respect."

ashurst

New "doxxing" offences under the PDPO

New PDPO offences	Two elements for offences:	"Specified Harm"
a) Two offences on doxxing (Section 63(4)); and b) Five offences related to non-compliance with or obstruction of investigative and enforcement powers exercised by the Privacy Commissioner (Section 66K onwards).	a) where a person discloses any personal data without the data subject's consent; and b) one of the following applies: (1) with the intention to threaten, intimidate, harass, or cause psychological harm to, the data subject or any immediate family; or (2) being reckless as to whether any specified harm would be (or likely to be) caused to the data subject (or data subject's family members).	a) harassment, molestation, pestering, threat or intimidation to the relevant person; b) bodily harm or psychological harm to the relevant person; c) harm causing the relevant person to be reasonably concerned for their well-being or safety; or d) damage to the relevant person's property.

ashurst

Two other impacts of PDPO Amendment Bill

Privacy Commissioner has new **direct criminal investigation and prosecution powers**, with most of these powers being exercisable beyond the doxxing offences (these powers are broadly similar to the takedown regime under the National Security Law).

Introduction of a "cessation notice" regime – Privacy Commissioner can compel takedown of content reasonably believed to be contravening doxxing offences, where the data subject is a Hong Kong resident or is present in Hong Kong at the time of disclosure.

ashurst

Recent "doxxing" data privacy developments

June 2022 - PDPC announced that it has issued more than 770 "cessation notices" to 14 social media platforms, for the removal of ~3,900 unlawful doxxing messages sent over the past eight months. -

May 2022 – PDPC has initiated the first prosecution against doxxing activities, charging a company director with illegally leaking the personal particulars of two people with whom he allegedly had a monetary dispute.

May 2022 – media speculation regarding banning of Telegram, per S66L of the PDPO (no direct comments from Government).

While the PDPO Amendment Bill purports to apply to overseas companies - difficult to assess how this can be enforced on an overseas entity that has no staff in Hong Kong, and restricting access to a platform in Hong Kong (without impacting other platforms) will also be difficult.

Recent “doxxing” data privacy developments (cont.)

"I would also urge the operators of social media platforms to discharge their own responsibility to monitor any unlawful content with regards [to], for example, doxxing messages on their platforms. And they should also take action to remove the unlawful doxxing messages right away if those messages appear on their platform."

ashurst

HK cross-border transfer model contractual clauses

- PCPD has published a Guidance on Recommended Model Contractual Clauses (the **RMCs**) for Cross-border Transfer of Personal Data (the **Guidance**) to facilitate the use of contractual clauses to satisfy the requirement in (not-yet-effective) section 33(2)(f).
- PCPD intends for the RMCs to be incorporated into general commercial agreements recommends that data users incorporate or adapt the RMCs into their commercial agreements to ensure adequate measures have been taken in respect of cross-border data transfers. The Guidance states that adoption of the RMCs will also serve to illustrate that the Due Diligence Requirement and all factors would be taken into account in case of any suspected or alleged breach of the PDPO, including the DPPs.
- As with the ASEAN Model Contractual Clauses – the RMCs cover two cross-border data transfer scenarios: (a) transfers from a data user to a data processor; and (b) transfers from a data user to another data user.
- The RMCs and MCCs are largely aligned - including imposing obligations on the transferee to only use the transferred data for the prescribed purpose, rights of data subjects and inspection rights of the transferee where data is transferred from a data user to a data processor.
- Article to come comparing the two regimes.

ashurst

New HK cybersecurity law?

- **Hong Kong does not have a stand-alone cybersecurity / cybercrime law.** There are certain legislative provisions relating to cyber crimes – including within the Crimes Ordinance, the Telecommunications Ordinance and laws related to obscenity and child pornography.
- As set out in recent Policy Address and public comments - Security Bureau is currently preparing a draft cybersecurity law for circulation to Legislative Council, aiming to be released for public consultation by end of this year.
- Cybersecurity can encompass many aspects – including crimes on computer networks, information security, data security, fraud and misinformation. Cybersecurity law will aim to define:

"the cybersecurity responsibilities of critical information infrastructure operators and to enhance the protection of the operation and data of Hong Kong's network systems and critical infrastructure information systems."

ashurst

New HK fake news law? Further amendments to PDPO?

- Government also (in May) announced they are working on "fake news" legislation.

  "The fake news law needs a lot of research, especially (on) how overseas governments are tackling this increasingly worrying trend of spreading inaccurate information, misinformation, hatred and lies on the social media."

- Potential further changes to the PDPO (i.e. changes that were discussed in addition to the "doxxing" amendment) – to be confirmed, no timing available yet.

ashurst

ashurst

Data privacy update: China

TRACY WANG
Counsel, China

Data privacy update: China

1 **More clarity under the Personal Information Protection Law ("PIPL"), seven months after its promulgation?**

2 **How do Chinese data privacy requirements interact with other cybersecurity requirements, e.g. "important data"?**

3 **Latest developments on the steps/ documentation required for cross border transfer of personal information**

ashurst

Latest developments on the steps/ documentation required for cross border transfer of personal information

Options for cross border transfer of personal data	Latest development – draft rules
1 Completing risk review by Cyberspace Administration of China ("CAC");	Mandatory security review required for: • critical information infrastructure operators' cross border transfer of personal data • other data processors – several applicable thresholds: 1 million / 100,000 / 10,000
2 Having standard contract clauses ("SCCs") with offshore data receiving parties; or	Some key contents set out in a draft regulation on cross border data transfer. SCCs remain unreleased.
3 Obtaining a personal information protection certification from an agency accredited by the CAC	Can be applied for intra-group transfer of personal data, or processing of personal data by an offshore entity of PRC data subjects on a cross border basis

ashurst

Data privacy update: Australia

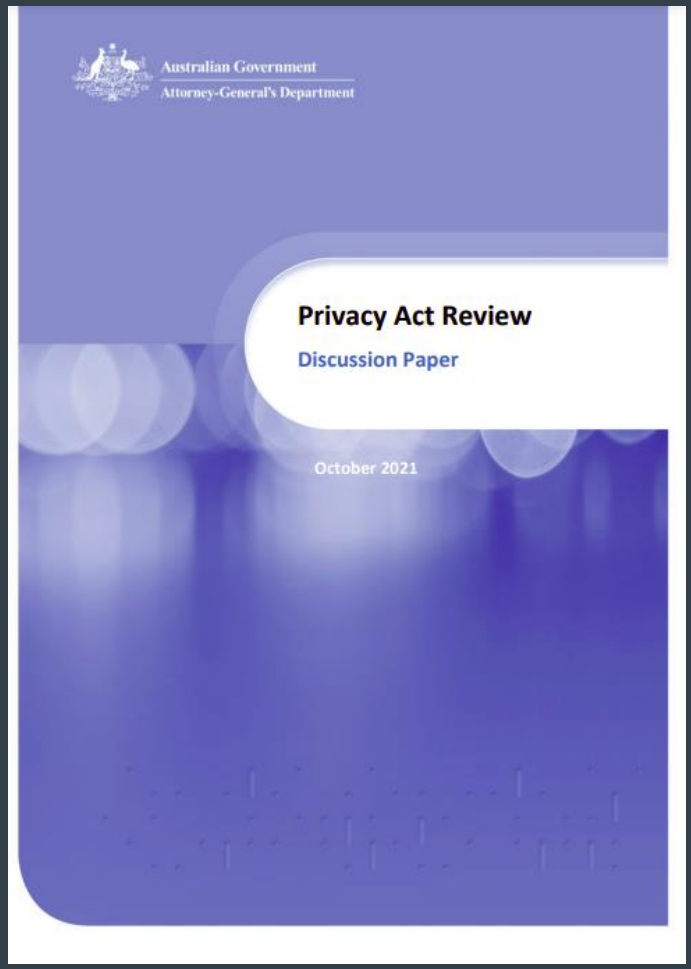
GEOFF MCGRATH
Senior Associate, Australia

Australia: Review of the Privacy Act

Major review of the Privacy Act underway

Some key areas of focus:

- Gaps in current law and 'high risk' practices
- More GDPR-like rules (but not adequacy)
- Cross border transfers: use of CBPR and (possibly) standard contractual clauses
- New rights and remedies, including direct right of action and statutory tort of privacy



ashurst

Australia: Recent cases and determinations

Extraterritorial application:

Facebook Inc v Information Commissioner [2022] FCAFC 9

- Installing cookies to deliver targeted advertising can be *carrying on business in Australia*

OAIC has already applied similar analysis in other contexts:

- Uber Technologies Inc
- Clearview AI

Facial recognition:

- 7-Eleven
- Clearview AI
- Australian Federal Police
- Retail Stores (Bunnings, Kmart and The Good Guys) under investigation

ashurst

Australia: What to look out for in the future

Themes we are seeing:

- Increasingly active regulator, although still underfunded
- Privacy concerns being regulated by other bodies (eg the ACCC)
- Recent regulator focus, Privacy Act review and related laws (eg CDR) has organisations reconsidering privacy compliance frameworks

Other recent/proposed laws and reviews:

- Consumer Data Right
- Online Privacy Bill
- Trusted Digital Identity Bill
- Data Availability and Transparency Act
- Review of Automated Decision and AI Regulation (March 2022)

ashurst

ashurst

Data privacy update: Singapore

EVAN LAM
Partner, Singapore

Amendments to the Personal Data Protection Regime

In force (as of 1 Feb 2021)

- Mandatory data breach notification
- Expansion to "deemed consent" concept / new exceptions
- New offences for individuals
- Preservation of personal data when processing access request

Not yet in force

- Data portability obligation
- Enhanced financial penalties

When to report

Significant harm

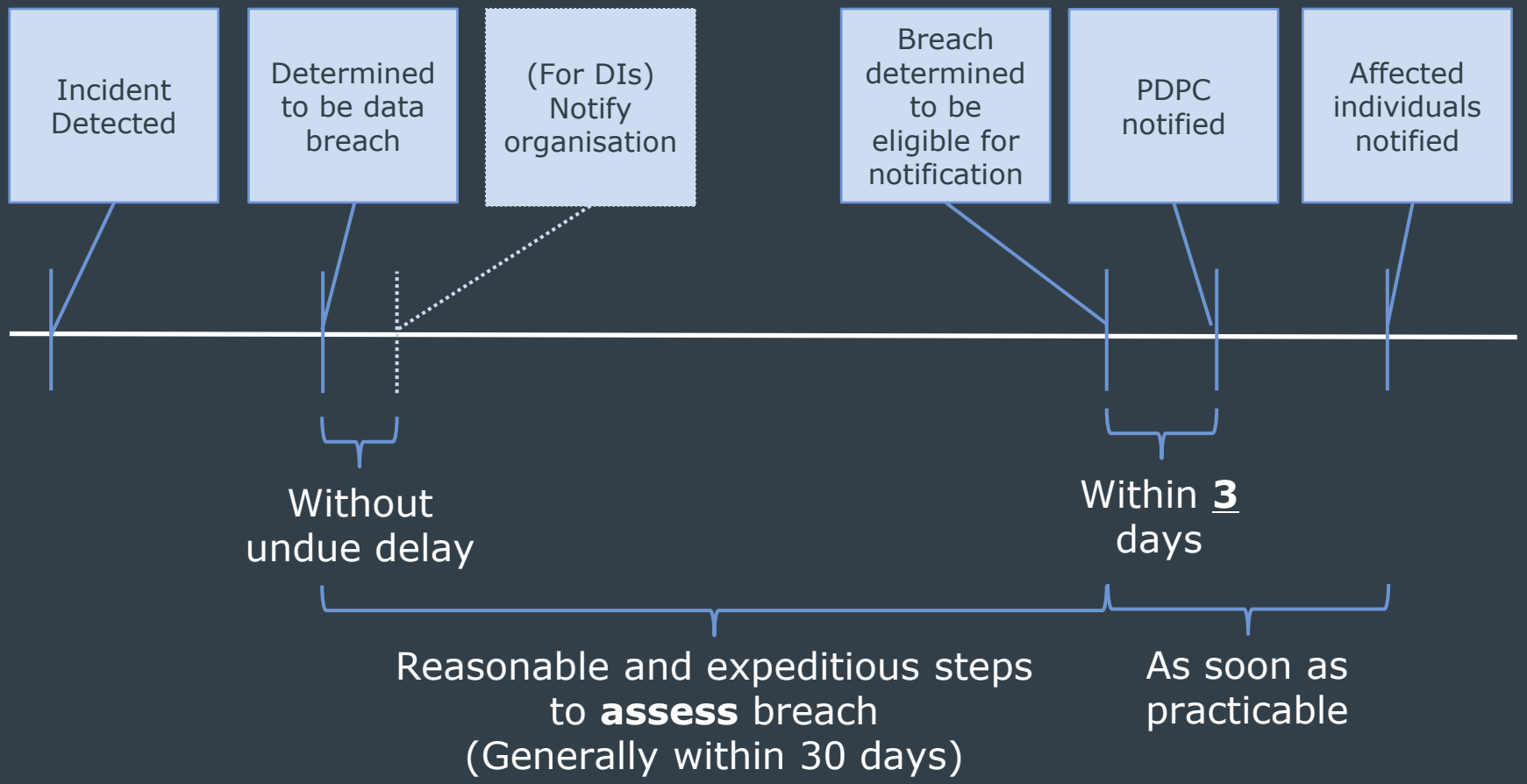
- Can include physical, psychological, emotional, economic, financial, reputational harm
- Prescribed categories of personal data
  - Personal Data Protection (Notification of Data Breaches Regulations) 2021

OR

Significant scale

- Affects 500 persons or more

Data Breach Reporting Timeline – Part VIA



Increased maximum penalties (Not in force)

Current position

- Individuals: S$200 million
- Organisations: S$1 million

OR

Amended position

- **Part III, IV, V, VI, VIA or VIB**
  - Annual turnover in Singapore of >$10 million – 10% of annual turnover in Singapore
  - Any other case – S$1 million
- **Part IX** (*DNC Registry*) or **s48B(1)** (*Dictionary attacks*)
  - Annual turnover in Singapore >$20 million – 5% of annual turnover
  - Any other case – S$1 million

Panel discussion: The future of data privacy in APAC

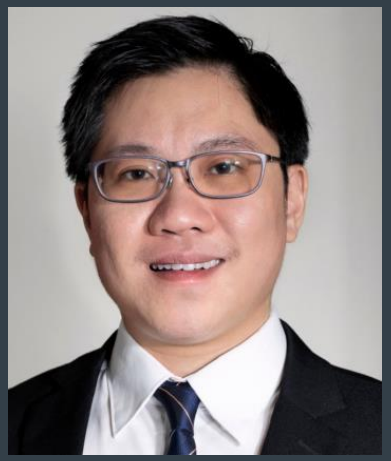
ashurst

Thank you

Hoi Tak Leung
Counsel
+852 2846 8982
hoitak.leung@ashurst.com

Tracy Wang
Counsel
+86 10 5936 2885
tracy.wang@ashurst.com

Geoff McGrath
Senior Associate
+61 3 9679 3816
geoff.mcgrath@ashurst.com



Evan Lam
Partner
+65 6602 9156
evan.lam@ashurst-adtlaw.com

ashurst