

Insights

PART 5 OF 6: AMENDMENTS TO HONG KONG DATA PROTECTION LAW TO WIDEN THE DEFINITION OF “PERSONAL DATA”

Jul 22, 2021

SUMMARY

Hong Kong proposes to widen the current definition of “personal data” to cover not just “identified” persons but also “identifiable” persons. The amendment is expected to cover the use of online tracking technologies such as internet cookies to the extent that they make it reasonably possible for persons to be identified.

This post is the fifth in the series of six articles in which we discuss the proposed amendments to the data protection regime in Hong Kong.

This post deals with that part of the proposed amendments to the Personal Data (Privacy) Ordinance (“PDPO”) that are aimed at widening the definition of “personal data”.

See links below for our previous articles on the proposed amendments:

- [Part 1 of 6: our first article set out an overview of the six proposed amendments and included a discussion of the proposed introduction of a mandatory data breach notification mechanism.](#)
- [Part 2 of 6: our second article on the requirement for the formulation of a clear data retention policy.](#)
- [Part 3 of 6: our third article on the imposition of administrative penalties.](#)
- [Part 4 of 6: our fourth article on the regulation of data processors.](#)

Introduction

There is no uncontested and thoroughly coherent definition for “personal data”. Jurisdictions around the world each adopt a definition which is thought to be most appropriate for their needs.

Hong Kong takes the view that it is important to adopt an appropriate definition of “personal data” which accords with the contemporary technologies in data analytics and data collection, so as to ensure that the data privacy law provides enough coverage to protect personal data.

In light of the increasing popularity in the use of tracking technology and data analytics, Hong Kong has proposed to widen the current definition of “personal data” under the Personal Data (Privacy) Ordinance (“PDPO”) to satisfy public expectation towards the protection of personal data.

The current definition and its deficiencies

Under the current PDPO, “personal data” means any information (a) relating to a living individual; (b) from which it is practicable for the identity of that individual to be ascertained; and (c) which comes in a form in which access to or processing of the information is practicable.

To put it simply, the PDPO currently covers personal data which relates to an actual living person whose identity can be ascertained, i.e. an “identified” person.

The existing definition of personal data does not cover situations where the data user has control of descriptions or identifiers which merely point to or are relatable to a person, i.e. data which relate to “identifiable” persons. With the use of modern data processing technologies, it has become possible for data users to link information such as residential addresses, IP addresses, and website cookies to identify persons. If this information held by a data user accretes so as to allow the identity of a person to be ascertained, it is thought by Hong Kong that such information should be regulated and protected under the PDPO.

Examples from other jurisdictions

The exact new definition for “personal data” has not yet been published. The Hong Kong government has taken reference from various overseas regulatory regimes which expressly regulate information relating to “identifiable” individuals, and likely will formulate a similar definition which aligns Hong Kong’s law broadly with current international standards.

Below are some examples of what other jurisdictions are regulating:

- Canada and New Zealand: information about “identifiable” individuals.
- Australia: information about “identified” individuals and individuals who are “reasonably identifiable”.
- The EU: information about “identified” and “identifiable” persons.

Note that Australia’s data privacy law distinguishes between individuals who are “potentially identifiable” and those who are “reasonably identifiable”. Only the latter falls under its definition of “personal information”. While it technically may be possible for a data user to identify an individual

from the collection of information it holds, the identification process required to identify an individual may come with an unreasonable cost or difficulty. If that is the case, the individual only is “potentially identifiable” and Australia has decided not to include this kind of information in its definition of “personal information”¹.

On the other hand, the GDPR of the EU regulates information relating to “an identifiable natural person”. It refers broadly to natural persons who, “directly or indirectly”, can be identified. The GDPR makes particular references to identifiers (such as names, location data and identifiers) and various factors specific to the identity of a person, but does not limit itself just to these identifiers. An element of reasonableness is present in the word “indirectly”. Indirect identification of an individual falls under the ambit of the GDPR if the data controller may identify an individual by using other information it holds or information it *reasonably* can access from another source. This is intended to add flexibility to the provisions so that it captures also technologies developed in the future which allow living persons to be identified in new ways.

Based on the above, we expect that an element of reasonableness likely will be present in Hong Kong’s new widened definition of “personal data” when it is made public.

What kind of information is expected to fall under the new definition?

On a practical level, what types of information are envisaged to be captured under the new definition?

In addition to the relatively straightforward personal identifiers, the GDPR expressly covers online identifiers which do not relate directly to living persons but rather relate to tools or digital footprints which may be traceable to individual persons. Recital 30 of the GDPR provides examples such as internet protocol (IP) addresses, website cookies and radio-frequency identification (RFID) tags. It appears from the Hong Kong government’s amendment proposals that these types of modern tracking and surveillance technologies also are on the radar.

Each of these named identifiers track different information. Each when viewed on its own may not fall under the ambit of “personal data”. However, when these identifiers together form a collection of online data of browsing preferences, habits and behaviours which becomes sufficient to point to a specific individual, we expect that such data will fall to be regulated under the new definition of “personal data”.

Points to take away

The definition of “personal data” under the PDPO is expected to be widened to include strands of non-personal information which together may enable persons to be identified. The new and widened scope of “personal data” will bring Hong Kong’s position into closer alignment with the current international standards.

Online behavioural tracking tools and identifiers commonly deployed by organisations that maintain websites likely will come within the purview of the Privacy Commissioner for Personal Data.

Businesses and organisations should update their privacy policies to ensure that any use of identifier or tracking tool is compliant with the established data protection principles.

1. For more discussion on Australia’s distinction between “potentially identifiable” individuals and “reasonably identifiable” individuals, see paragraphs 6.53 to 6.60 of ALRC Report 108 published by the Australian Law Reform Commission.

RELATED PRACTICE AREAS

- Data Privacy & Security
- General Data Protection Regulation
- Corporate

MEET THE TEAM



Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com

[+852 3143 8450](tel:+85231438450)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

