CII Hong Kong Webinar
Insurtech for Non-Life Insurers: Challenges, Risks & Data Privacy

Henry Wong
Founding Partner
WMC Partners, Solicitors, HKSAR
28 October 2020

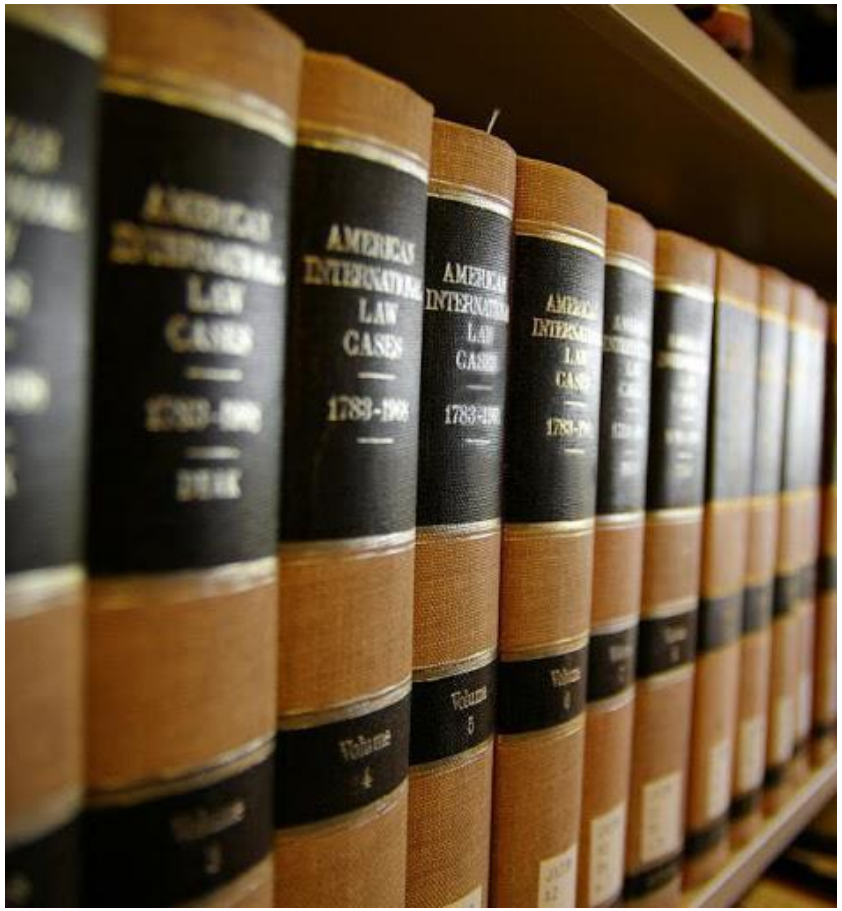
WMC Partners
黃麥朱律師行

Insurtech & Data Privacy

- *Introduction*
- *Some Key Sanctions for Breaches*
- *Illustrative Potential Vulnerabilities*
- *Judgments of Interest*
- *"Fruit" for Thoughts*

WMC Partners
黃麥朱律師行

Introduction

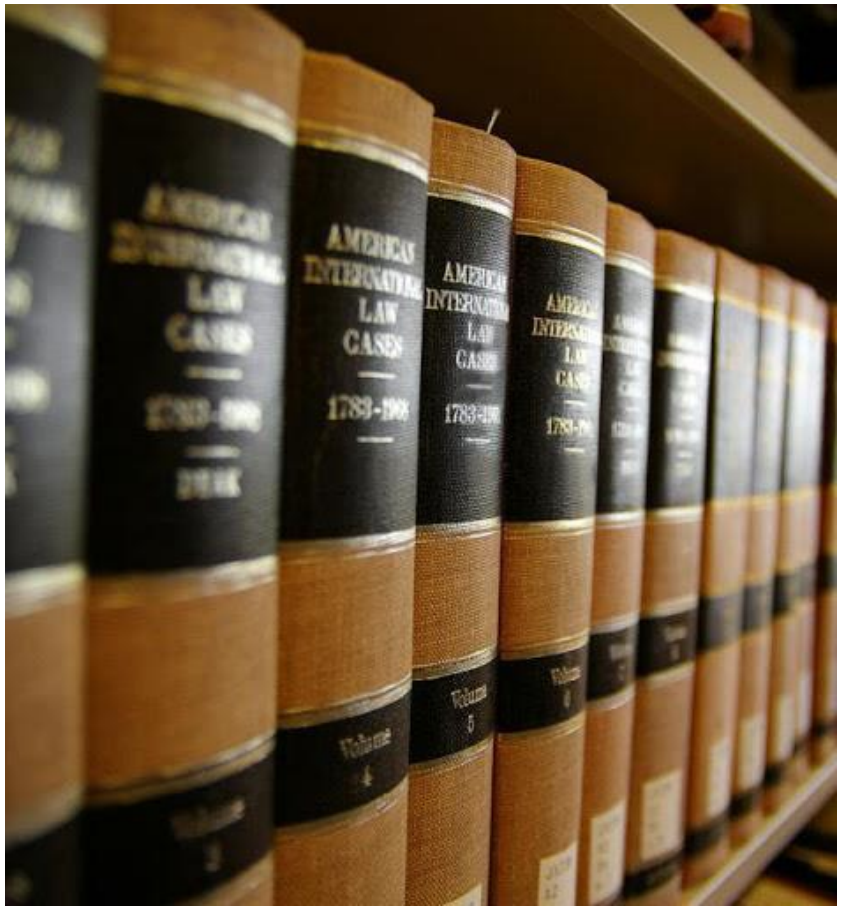


Introduction

The Personal Data (Privacy) Ordinance ("**PDPO**"), Cap. 486:

- commencement: *20 December 1996*;
  - to ensure an adequate level of data protection;
  - to retain Hong Kong's status as an international trading centre; and
  - to give effect to human rights treaty obligations.

N.B. Based on *the Development Privacy Guidelines 1980* of the *Organisation for Economic Co-operation*, which has 34 member countries such as Australia, Japan, Spain, United Kingdom and more.

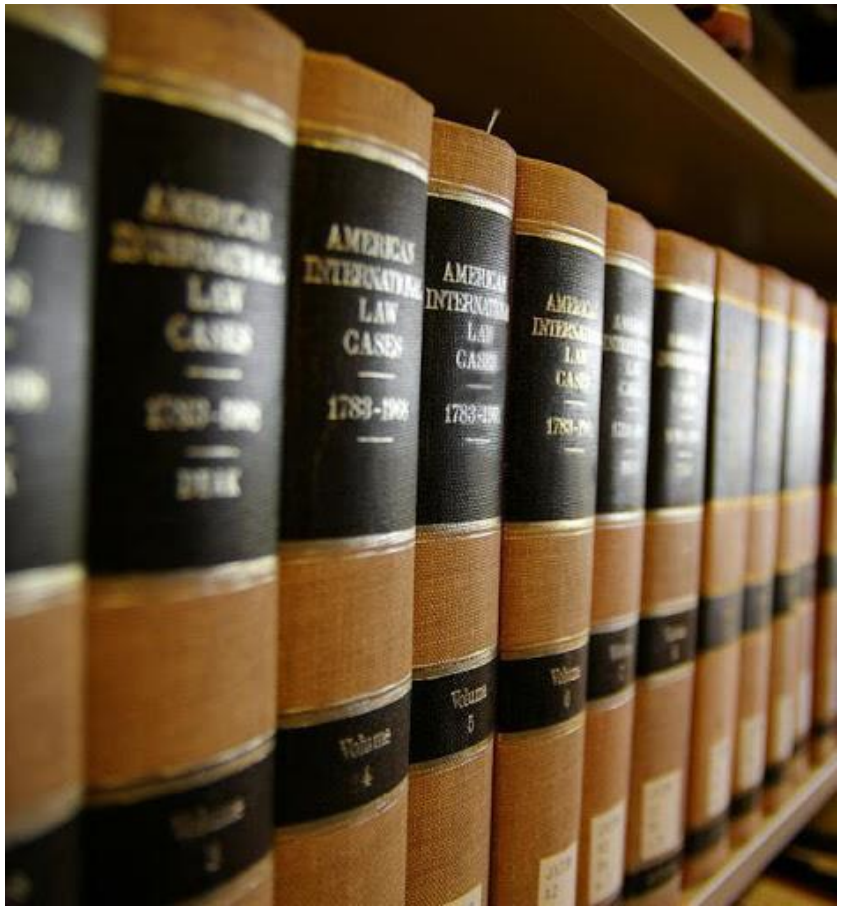


Introduction (cont'd)

Section 35 (came into force 25 April 2013):

To curb new privacy challenges and brought in new and more severe sanctions. Some key coverages are:

- Data user to take specified actions before using personal data in direct marketing: ***Section 35C*** ;
- Data user to take specified actions before providing personal data to another person: ***Section 35J*** ;
- Data user must not provide personal data for use in direct marketing without data subject's consent: ***Section 35K*** .



Introduction (cont'd)

- In 2018,
  - there were 16,875 enquiries and 1,890 complaints received, including e.g. those related to the leakage of passengers' personal data by Cathay Pacific Airways; and
  - in 2018-2019 there was a 19.6% rising proportion of inadequate security;

- Per Privacy Commission's records, just in 2018, 9.8 million individuals were affected by data privacy breaches in the HKSAR.

Sources: South China Morning Post and Hong Kong Free Press

Privacy watchdog played the role as "friendly" regulator

	2014	2015	2016	2017	2018
Data breach incidents reported	**70**	98	**89**	106	**129**
Privacy watchdog initiated investigations	**106**	76	**4**	1	**4**
Enforcement notices issued	**90**	67	**6**	3	**0**
Warnings	**20**	17	**36**	26	**16**
Compliance checks completed	**219**	279	**259**	253	**289**
Complaints received	**1,702**	1,971	**1,838**	3,501*	**1,890**

**1968 complaints in 2017 concerned with electoral office losing two laptops, that aside, there were 1,533 complaints*

SCMP
Source: Privacy Commissioner for Personal Data

Some Key Sanctions for Breaches

Some Key Sanctions for Breaches

- **section 35C (5)**

  A data user who uses a data subject's personal data in ***direct marketing without taking each of the actions specified in subsection (2)*** commits an offence and is liable on conviction to a fine of $500,000 and to imprisonment for 3 years

Some Key Sanctions for Breaches

- **section 35D (2)**

  a) **inform** the data subject-

  (i) that the data user intends to so use the personal data; and

  (ii) that the data user may not so use the data unless the data user has received the data subject's **consent** to the intended use;

  b) **provide** the data subject with the following information in relation to the intended use—

  (i) the **kinds** of personal data to be used; and

  (ii) the classes of marketing subjects in relation to which the data is to be used; and

  c) **provide** the data subject with a **channel** through which the data subject may, without charge by the data user, **communicate** the data subject's consent to the intended use.

Some Key Sanctions for Breaches

- **section 35J (5)**

  A data user who provides personal data of a data subject to another person for use by that other person in **direct marketing** without taking each of the actions specified in subsection (2) commits an offence and is liable on conviction:

  a) if the data is provided for gain, to a fine of $1,000,000 and to imprisonment for 5 years; or

  b) if the data is provided otherwise than for gain, to a fine of $500,000 and to imprisonment for 3 years.

Some Key Sanctions for Breaches

- **section 35K** (1)

  A data user who has complied with section 35J must not provide the data subject's personal data to another person for use by that other person in **direct marketing** unless –

  a) the data user has received the data subject's **written consent** to the intended provision of personal data, as described in the information provided by the data user under section 35J(2)(b), either generally or selectively;
  b) if the data is provided **for gain**, the intention to so provide was specified in the information under section 35J(2)(b)(i); and
  c) the provision is consistent with the data subject's consent.

Some Key Sanctions for Breaches

- **section 35K (4)**

  A data user who contravenes subsection (1) commits an offence and is liable on conviction— (a) if the data user provides the personal data for gain, to a fine of $1,000,000 and to imprisonment for 5 years; or (b) if the data user provides the personal data otherwise than for gain, to a fine of $500,000 and to imprisonment for 3 years.

WMC Partners 黃麥朱律師行

Some Key Sanctions for Breaches

- **Section 50A**

  if a data user breaches **an enforcement notice** issued by the Privacy Commissioner,

  a) on a first conviction:

  (i) to a fine at level 5 and imprisonment for two years;

  (ii) if the offence continues after the conviction, to a daily penalty of $1,000; and

  b) on a second or subsequent conviction:

  (i) to a fine at level 6 and to imprisonment for 2 years; and

  (ii) if the offence continues after the conviction, to a daily penalty of $2,000.

WMC Partners 黃麥朱律師行

Illustrative Potential Vulnerabilities

WMC Partners 黃麥朱律師行

Potential Vulnerabilities

- **Health Insurance:**
  - Customized model of healthcare inevitably creates and stores large amount of specific genetic and lifestyle information of certain population for the purposes of e.g. creating personalized treatment plans.
  - The management and transfer of this big pool of data would creates avenues for potential future large liability issues as the amount of data needed to create a customized personal model is enormous.
  - The more and more commonly adopted cloud-based storage of those enormous pool of data in turn would create concerns about confidentiality and privacy in e.g. data transfers from one platform to another, or along various hubs in the blockchain matrix.

Source: KPMG

Potential Vulnerabilities

- **Autonomous Vehicles:**
  - With or without further motor insurance elements to add on, the new generation of automobiles is already collecting and storing significant amounts of personal data from individuals. In due course, more and more of those data would likely be utilized by motor underwriters on setting premium and/or decision on taking or rejecting the risks.
  - Data now collectable and hence stored includes, e.g. geo-location data from navigation systems, driver behavior patterns (for monitoring speed limits compliance), integration with cell phones who at the same time would help insurers to analyze more personalized insurance products, premium adjustment tools etc.
  - Like different parts of any car, some of those products are provided by third parties which could lead to intentional or even unintentional breaches of the provisions under PDPO.
  - Non-life insurance products like traditional personal accident insurance, product liability insurance and business interruption insurance needed to cover potential breaches of personal data collected by insurance companies.

Source: KPMG

Judgments of Interest

Some Relevant Judgments – HK - US

Case 1:19-cv-07859-JSR Document 1 Filed 08/21/19 Page 1 of 13

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SS&C TECHNOLOGIES HOLDINGS, INC. Plaintiff, v. AIG SPECIALTY INSURANCE COMPANY, Defendant.	Civil Action No.: 19-cv-7859 **COMPLAINT** **JURY TRIAL DEMANDED**

SS&C Technologies Holdings, Inc. ("SS&C"), by and through its undersigned attorneys, as and for its Complaint against AIG Specialty Insurance Company ("AIG"), alleges as follows:

WMC Partners 黃麥朱律師行

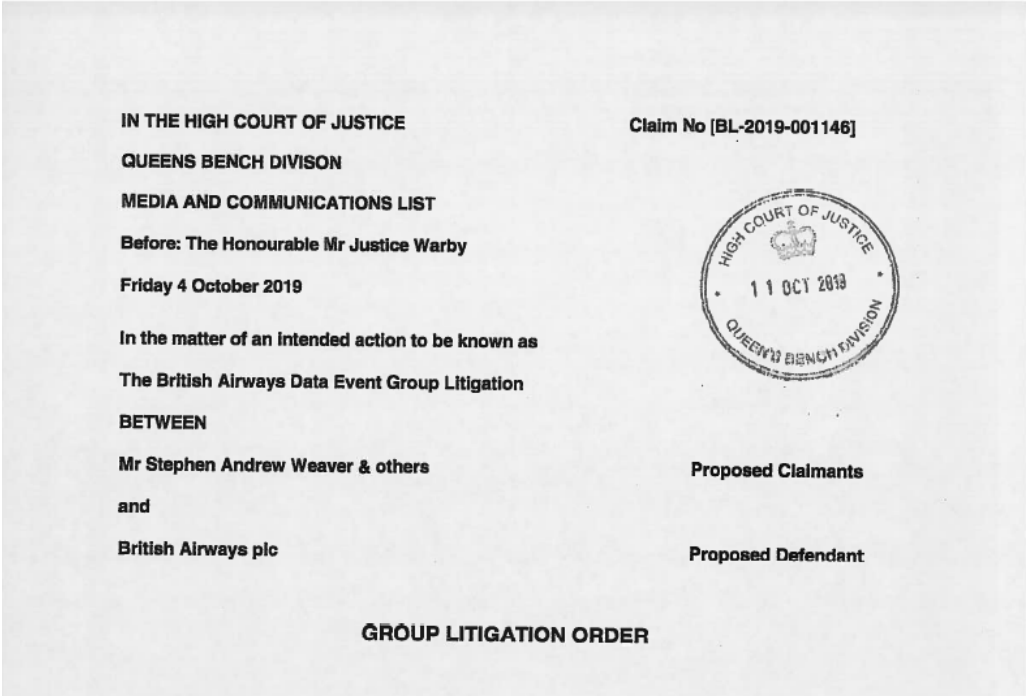
Some Relevant Judgments – HK - US

- In *SS&C Tech. Holdings, Inc v AIG Specialty Ins. Co*, SS&C Technologies was involved in a major cyber incident in which Chinese hackers managed to dupe the company out of US$5.9 million. Spoof emails purporting to come from one of the company's clients – Tillage Commodities Fund – instructed the company to make six wire transfers to an unknown bank account holder in Hong Kong.
- AIG says it never sold the company a "cyber insurance" policy. AIG says that it insured SS&C under a "specialty risk protector policy of insurance." In the middle of the policy was a clause that AIG did not agree to provide indemnity coverage for losses arising from "dishonest, fraudulent or criminal acts."
- AIG agreed to pay the defense costs for those cases, but not the actual losses.
- SS&C Technologies has already acknowledged that the funds were "stolen" and not "lost."
- The Chinese criminals stole the $5.9 million from a client account, and therefore, the insurance policy did not apply, and SS&C has no right to demand payment for the claim.

Some Relevant Judgments - HK

- On 18 October 2010, the Privacy Commissioner found that Octopus had unauthorised collection of data such as Hong Kong identity card number, passport number, birth certificate number as well as month and year or birth.
- Octopus did not take all reasonable steps to inform its customers of the classes of persons to whom the personal data may be transferred as it was in vague terms and partly because the Personal Information Collection Statement was printed in unreasonably small font.
- The Privacy Commissioner also held that customers' personal data was shared with business partners for monetary gain without the consent of Octopus's customers.
- Under the Ordinance as it stood before the amendments made in 2013, a breach of a data protection principle is not an offence and only an enforcement notice on a party can be.
- However Octopus had ceased or suspended all arrangements with business partners to sell customers' personal data and had undertaken to implement various changes to its practices.

Some Relevant Judgments - UK



IN THE HIGH COURT OF JUSTICE
QUEENS BENCH DIVISON
MEDIA AND COMMUNICATIONS LIST
Before: The Honourable Mr Justice Warby
Friday 4 October 2019

Claim No [BL-2019-001146]

HIGH COURT OF JUSTICE
11 OCT 2019
QUEEN'S BENCH DIVISION

In the matter of an intended action to be known as
The British Airways Data Event Group Litigation
BETWEEN
Mr Stephen Andrew Weaver & others — Proposed Claimants
and
British Airways plc — Proposed Defendant

GROUP LITIGATION ORDER

- GDPR gives data regulators the power to fine up to €20m (£18m), or 4% of annual global turnover, whichever is greater.
- For example, British Airways, which cooperated with the ICO investigation, was fined 1.5% of its global turnover. Had ICO sought the maximum fine of 4% of BA's total revenue, the bill could have been £489m.

WMC Partners 黃麥朱律師行

Some Relevant Judgments - UK

- British Airways' announced that the personal and financial details of customers making bookings on its website and app between 21st August and 5th September 2018 had been hacked. The hacked information included customers' names, email addresses and credit card details.
- The hack included diverting user traffic from the British Airways website to a fraudulent site, where customer details were harvested by hackers.
- The ICO also found that that the data breach was more extensive than previously reported, affecting approximately 500,000 customers and had begun in June 2018. The ICO announced its intention to fine British Airways £183.39 million for a breach of the General Data Protection Regulation (GDPR) in relation to the serious data hack.
- Fines received by the ICO go back to the Treasury. However, the ICO is exploring options, including ringfencing part of the fine income to cover potential litigation costs to defend its decisions.

Some Relevant Judgments - UK

Hilary Term
[2020] UKSC 12
On appeal from: [2018] EWCA Civ 2339

JUDGMENT

WM Morrison Supermarkets plc (Appellant) *v*
Various Claimants (Respondents)

before

Lady Hale
Lord Reed
Lord Kerr
Lord Hodge
Lord Lloyd-Jones

JUDGMENT GIVEN ON

1 April 2020

Heard on 6 and 7 November 2019

WM Morrisons Supermarket Plc v Various Claimants [2018] EWCA Civ 2339, upheld the finding of the High Court that an employer can be vicariously liable for an employee's data breach even when the employer was not at fault.

In response to an argument put forward by Morrisons that public policy considerations militate against imposing a disproportionate burden on an employer, the Court of Appeal's response was that "*the solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees*". It deals with liability and not with quantum.

However, the data of almost 100,000 employees leaked and any awarded compensation, including distress based damages, will likely be considerable.

Some Relevant Judgments - UK

- On November 30, 2018, Marriott International announced that an "unauthorized party" gained access to the personal information of 500 million Starwood customers. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident. It was then discovered that this party had copied and encrypted customer information and acted towards removing it from the Starwood database as early as 2014.
- The lawsuit, which seeks unspecified damages for loss of control of personal data, automatically includes guests who made a reservation for one of the former Starwood brand hotels before 10 September 2018.
- In July 2019, ICO has issued a notice of its intention to fine Marriott International £99,200,396 for infringements of the GDPR.
- In January 2020, Marriott International has confirmed it has suffered a second data breach, compromising the personal data of roughly 5.2 million guests. The breach may have taken personal details such as names, birthdates, and telephone numbers, along with language preferences and loyalty account numbers.

“Fruit” for Thoughts

- ✓ Insurtech shaping the future of General Insurance.
- ✓ The ABCD of Insurtech in a big data, cross institutional and cross discipline blockchain matrix.
- ✓ Personal Data Protection is just but one aspect which General Insurers could not overlook when shaping the business model for tomorrow.
- ✓ Infringing Personal Data Protection laws, as demonstrated by the BA and Marriott cases, just the penalties could be devastating.
- ✓ Potential reputational damage.
- ✓ Also risk law suits from shareholders’ for possible breach of directors’ duties.
- ✓ If HK would follow UK to make the 2018 amendments to PDPO, or claimant could choose UK to bring law suits, the monetary damage would be huge.

****

- *Acknowledgments*

- *Personal Data Privacy Ordinance*
- *KPMG*
- *Hong Kong Free Press*
- *South China Morning Post*

Stay Healthy to conquer covid-19 together!

WMC Partners
黃麥朱律師行