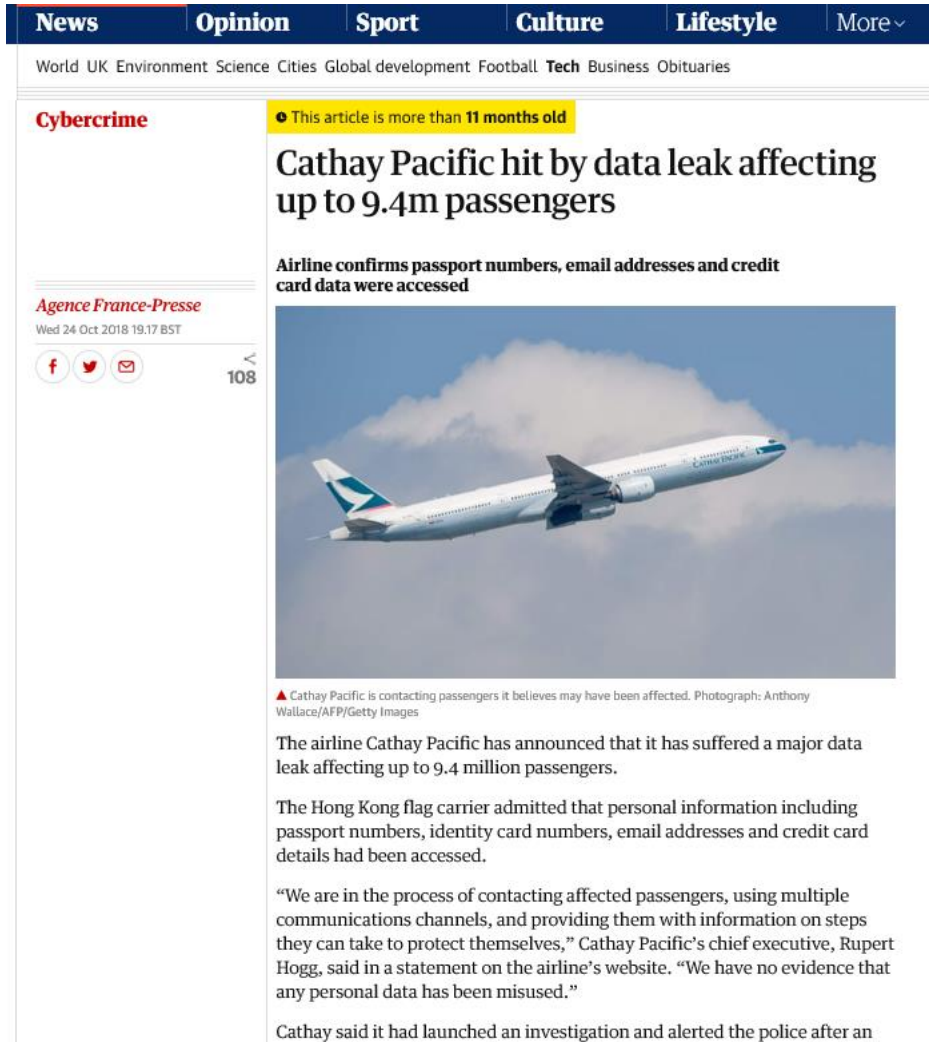
HONG KONG

Hong Kong

- **9.4 million** impacted passengers
- It took Cathay Pacific **7 months** to alert passengers of the data leak
- The PDPO **does not require** organisations to **notify** the PCPD or impacted data subjects after they discover a data security breach
- The PCPD's investigation focused on Cathay Pacific's compliance with the obligation that data users take all reasonably practicable steps to protect personal data against unauthorised access (the PCPD found that Cathay Pacific was in breach of this obligation)
- **No fine**, just an **enforcement notice**
- May lead to PCPD introducing a mandatory data breach notification obligation to the PDPO



News Opinion Sport Culture Lifestyle More

World UK Environment Science Cities Global development Football Tech Business Obituaries

Cybercrime

This article is more than 11 months old

Cathay Pacific hit by data leak affecting up to 9.4m passengers

Airline confirms passport numbers, email addresses and credit card data were accessed

Agence France-Presse

Wed 24 Oct 2018 19.17 BST

108

▲ Cathay Pacific is contacting passengers it believes may have been affected. Photograph: Anthony Wallace/AFP/Getty Images

The airline Cathay Pacific has announced that it has suffered a major data leak affecting up to 9.4 million passengers.

The Hong Kong flag carrier admitted that personal information including passport numbers, identity card numbers, email addresses and credit card details had been accessed.

"We are in the process of contacting affected passengers, using multiple communications channels, and providing them with information on steps they can take to protect themselves," Cathay Pacific's chief executive, Rupert Hogg, said in a statement on the airline's website. "We have no evidence that any personal data has been misused."

Cathay said it had launched an investigation and alerted the police after an

[IDPL Ch 4 ‘Hong Kong SAR – New Life for an Established Law’]

Hong Kong SAR

- *Context*: A liberal but only partly democratic SAR of the PRC; strong rule of law and non-corrupt courts.
  - 2019 crisis over extradition law & PRC hostility to democracy
- APEC & APPA member; not part of APEC-CBPR
- Basic Law provides constitutional protection
  - Used to find telecommunications surveillance unlawful
- No common law privacy right or extended confidence
- *Personal Data Protection Ordinance* 1996
  - Combination of EU, OECD and UK influences: first comprehensive data protection law in Asia
  - Privacy Commissioner for Personal Data (PCPD): first 'European' model of a DPA in Asia
- *Amendment Ordinance 2012 (in force April 2013)*
  - first significant change in 15 years; strengthens Act
  - fewer changes than Privacy Commissioner proposed

Hong Kong SAR – Principles (1)

- HK Ordinance covers all basic principles
  - *Eastweek v PCO* (2000): CA limited meaning of 'personal data' to exclude data collected without intention to identify (even though data otherwise sufficient for identification)
- Additional principles (stronger than OECD basics)
- 'Publicly available information' is still 'personal data'
  - *'Do No Evil' s48(2) decision* (2013) – government purpose (express or implied) limited use, not company's purpose (p96); controversial eg Deane (Deacons)
  - All public registers may have some implied limits on use
- Collection by 'unfair' means
  - *Sudden Weekly decision* upheld by AAB (p95) – Media intrusive practices were in breach, as 'unfair'; *Campbell* distinguished; public figures have some privacy in HK
  - 'Blind' 'recruitment' advertisements used to gather personal data

Hong Kong SAR – Principles (2)

- Deletion required
  - Hang Seng Bank decision: reduced holding bankruptcy data from 99 years to 8 years
- Data matching controlled
  - PCPD authorisation required if comparing more than 10.
- Direct marketing severely restricted
  - Pre-2012, mere opt-out at time of marketing required
  - Post-2012, consent to own marketing use must be obtained in advance (Part VIA); US$64K fine (p100)
  - For sale to others, similar opt-in, but fines up to US$125K.
- Voluntary data breach notifications (all sectors)
  - 61 DBNs 2012-13; compliance check follows in all cases
- ID numbers have largely unlimited use in public sector (except for data matching), and for avoidance of non-trivial losses in private sector
  - PCPD vigilance/complaints prevents unrestricted private sector use (p 104)
- s33 data export limitations (not in force) - no effective export limits– 2014 draft Guidelines not followed-up; Cannot bring into force – applies to PRC mainland

HK Amendment Ordinance 2012 Enforcement (1)

- PCPD powers still limited: cannot fine or compensate
  - *Cathay Pacific data breach re 9.4M people* (2019 Update p. 18): PCPD found numerous breaches, but could not fine or compensate; compensation cases before HK courts possible; potential GDPR extra-territorial liability
- PCPD's compliance notices (on complaint or own motion)
  - PCPD can direct a data user to remedy a breach, and specify how
  - No longer any need for likelihood of continuation before notice
  - Failure to comply is now an offence
  - Repeating the same breaches also now an offence (ADPL p.109)
- Offences
  - Pre-2012, penalties for non-compliance were derisory
  - First jail sentence (4 weeks) for misleading PCPD (Dec 2014)
- Rights of appeal to AAB
  - Complainants can appeal to Administrative Appeals Board against failure of PCPD to issue enforcement notice, or failure to investigate
- Compensation cases before courts
  - District Court can award damages under s66, including for injury to feelings;
  - Full defence if D can show 'reasonable care', or inaccurate data from 3rd P
  - Since 2012, PCPD can assist with preparation of case, or providing legal aid (repaid from damages; no evidence this has been utilised.

Hong Kong – Enforcement (2)
Post-2014 decline?

- *2017 Update* pp.11-12: apparent decline in enforcement & transparency since 2014; *2019 Update* p.18 indicates reversal
  - New Commissioner 2015; hosted ICDPPC 2017 (distraction).
- Transparency?
  - Use of s48(2) 'name & shame' reports resumed; now 5 since 2015.
  - AAB appeal decision summaries resumed; most in Chinese only.
  - Case Notes resumed and updated; around 15 p/a.
  - Media statement on contentious issues were often Chinese-only, but during 2019 crisis in English as well.
- Enforcement?
  - Two August 2018 prosecutions of Hutchison Telecom for failure to observe direct marketing opt-out: HK$20K fine (A$4K)
  - Hundreds of current cases of 'doxing' of both police and protesters
    - PCPD has no power to order 'take downs' or obtain injunctions; can only request
    - PCPD has referred 692 cases to Police for possible prosecution
  - Cathay Pacific data breach demonstrates weaknesses most clearly

Result: Transparency restored, but enforcement powers now obviously too limited; no longer one of Asia's leading jurisdictions