

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

**Computer Law
&
Security Review**

Asia-Pacific news[☆]



Gabriela Kennedy

Mayer Brown JSM, Hong Kong

A B S T R A C T

Keywords:

Asia-Pacific
IT/information technology
Communications
Internet
Media
Law

This column provides a country by country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia-Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

© 2014 Mayer Brown JSM. Published by Elsevier Ltd. All rights reserved.

1. Hong Kong

1.1. Privacy Commissioner condemns the collection of HKID Card copies and date of birth information by a fitness centre

The Privacy Commissioner for Personal Data published an investigation report on 5 December 2013, and issued an Enforcement Notice against fitness centre chain California Fitness, for excessive collection of personal data from its customers, including HKID Card copies and full date of birth particulars. This article will look at the key findings of the investigation report and discuss the practical implications of the decision.

1.1.1. Summary of the investigation report

California Fitness ("CF") is a fitness centre chain which provides fitness training and facilities in Hong Kong. At present CF has eight branches.

1.1.1.1. *Personal data involved.* Two CF customers complained to the Privacy Commissioner that CF had requested excessive personal data from them when one of them applied

for membership with CF and the other sought to renew his membership with CF. The personal data involved were:

- (i) Hong Kong Identity Card ("HKID Card") numbers;
- (ii) copies of HKID Cards (one of the complainants refused and instead provided a copy of his Home Visit Permit); and
- (iii) date of birth information (year, month and date).

The Privacy Commissioner launched an investigation. The investigation report revealed that CF started collecting such data in 2007. As of July 2013, CF had in excess of 200,000 copies of HKID Cards of members.

1.1.1.2. *Applicable data protection principle.* The case revolves around the requirements of Data Protection Principle (1) ("DPP(1)") of the Personal Data (Privacy) Ordinance ("PDPO"). DPP(1) stipulates that the collection of personal data must be necessary for the intended purpose. The personal data collected must not be excessive.

In addition, the "Code of Practice on the Identity Card Number and other Personal Identifiers" issued by the Privacy Commissioner in 1997 requires that a data user must not collect HKID Card numbers or copies of HKID Cards except

[☆] Gabriela Kennedy (gabriela.kennedy@mayerbrownjms.com) Partner, Mayer Brown JSM and member of the CLSR Professional Board (Tel: +852 2843 2211). For further information about Mayer Brown JSM see: www.mayerbrown.com. 0267-3649/\$ – see front matter © 2014 Mayer Brown JSM. Published by Elsevier Ltd. All rights reserved. <http://dx.doi.org/10.1016/j.clsr.2014.02.003>

under limited circumstances specified in the Code, e.g. where the collection is expressly authorized by law or where the collection is for the prevention or detection of crime or seriously improper conduct. The Code is not legally binding but a breach of the Code will give rise to an unfavourable presumption against the data user in legal proceedings.

1.1.1.3. *The Privacy Commissioner's findings.* CF put forward a number of explanations for requesting such personal data from its customers. While the collection of HKID Card numbers was justified under the Code (to establish a legal right or interest or liability on the part of the data subject), the collection of copies of HKID Cards and of full birth date particulars were found to amount to an excessive collection of data and thus be in breach of DPP(1) and the Code.

(i) HKID Card numbers

CF explained that in light of past cases of unpaid fees or damage to equipment or facilities by members, CF inserted its customers' HKID Card numbers in the membership contracts to facilitate the enforcement of contract. The report revealed that CF lodged more than 2800 civil claims between 2005 and 2008 against its customers. Considering that the potential loss or liability under the membership contracts was not of a transient or trivial nature, the Privacy Commissioner found that CF's collection of HKID Card numbers for inclusion in membership contracts was justified.

(ii) Copies of HKID Cards/Home Visit Permits

CF claimed that keeping the HKID Card copies of its customers could facilitate its internal administration and external audit. In addition, CF submitted that the collection of HKID Card copies would discourage its staff, who earn commission based on new memberships, from fraudulently creating membership accounts.

Those arguments were rejected and the Privacy Commissioner reiterated that stricter control is applicable to the collection of HKID Card copies, the misuse of which would be more likely to create opportunities for forgery or identity theft. The Privacy Commissioner was not persuaded by the evidence before him that the passive retention of HKID Card copies by itself could effectively monitor or deter any fraudulent activities. The Privacy Commissioner considered alternative means could be employed which would be less privacy-intrusive, e.g. randomly checking employee records or making calls to members to verify their application. The Privacy Commissioner was also not persuaded that the HKID Card copies by themselves would be necessary for audit purposes, since auditors could verify CF's income from other sources such as CF's bank statements or by seeking confirmation from banks.

Since Home Visit Permits contain similar sensitive personal data of individuals, the same restrictions would apply to the collection of Home Visit Permits.

(iii) Birthday information (year, month and date)

CF argued that the collection of the date of birth information was necessary for CF to offer birthday privileges and

promote age-specific products to members. The Privacy Commissioner found that the collection of the month of birth would be sufficient for birthday privilege purposes, and that the mere inspection of a HKID Card would do if CF wanted to promote age-specific products. CF had no justification to seek the collection of full date of birth particulars.

1.1.1.4. *Outcome.* The Privacy Commissioner found CF to have breached DPP(1) as it collected HKID Card copies and full date of birth particulars from its customers. An Enforcement Notice was issued to direct CF to remedy and prevent any recurrence of the contravention.

1.1.2. *Implications*

The investigation report may not be the final word on this story. It is understood that CF has filed an appeal to the Administrative Appeals Board against the Privacy Commissioner's decision.

Regardless of the outcome of the appeal, this case serves as a timely reminder that data users must think twice before collecting HKID Card (and other identification documents) information/copies and exact birthday information from individuals. While DPP(1) and the Code have been effective for over 15 years, in recent cases the Privacy Commissioner has demonstrated his increasingly strong disapproval towards the excessive collection of personal data (especially after the Octopus card incident) and the inclination to fully investigate complaints that relate to the excessive collection of personal data, in particular any collection of HKID Card copies (as such data is deemed "sensitive" by the Privacy Commissioner).

A few practical tips for data users:

- The PDPO does not impose an absolute ban on the collection of HKID Card copies and the other personal data concerned in this case. However, data users should have the default mind-set that they should not collect such personal data unless the collection can be justified within the meaning of the PDPO and the Code (merely administrative convenience or costs-saving is unlikely to amount to a good and valid reason).
- Data users should always consider alternative means which would be less privacy-intrusive. For example, where the customer submits his/her application in person, his/her identity can be verified on the spot without the need to retain any copy of the identification submitted.
- When responding to an investigation by the Privacy Commissioner, data users must be able to justify the purposes of collection of such data with adequate evidence. For example, where the collection is required by a third party (like an external auditor or a bank), the data user should be able to have such statements corroborated by such third parties. Another example is where it is alleged a particular measure is necessary to control or prevent some improper conduct (like employee/customer fraud), supporting evidence in the form of statistics showing the effectiveness of the measure (e.g. number of fraud cases before and after the measure) would be helpful.
- All data users who are currently collecting HKID Card copies and full date of birth of customers/members should take this opportunity to review their practices and policies.

Download English Version:

<https://daneshyari.com/en/article/466712>

Download Persian Version:

<https://daneshyari.com/article/466712>

[Daneshyari.com](https://daneshyari.com)