THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FIFTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Fifth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2018
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGER
Pere Aspinall

ACCOUNT MANAGERS
Jack Bagnall, Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Keavy Hunnigal-Gaw

EDITORIAL COORDINATOR
Thomas Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-62-1

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

BTS&PARTNERS

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

M&M BOMCHIL

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 12

HONG KONG

Yuet Ming Tham[1]

I OVERVIEW

The Personal Data (Privacy) Ordinance (PDPO) establishes Hong Kong's data protection and privacy legal framework. All organisations that collect, hold, process or use personal data (data users) must comply with the PDPO, and in particular the six data protection principles (DPPs) in Schedule 1 of the PDPO, which are the foundation upon which the PDPO is based. The Office of the Privacy Commissioner for Personal Data (PCPD), an independent statutory body, was established to oversee the enforcement of the PDPO.

Hong Kong was the first Asian jurisdiction to enact comprehensive personal data privacy legislation and to establish an independent privacy regulator. Unlike the law in several other jurisdictions in the region, the law in Hong Kong covers both the private and public sectors. Hong Kong issued significant new amendments to the PDPO in 2012 with a key focus on direct marketing regulation and enforcement with respect to the use of personal data.

Despite Hong Kong's pioneering role in data privacy legislation, the PCPD's level of activity with respect to regulatory guidance and enforcement has been relatively flat in the past year. In addition, Hong Kong has not introduced stand-alone cybercrime or cybersecurity legislation as other Asian countries have done. Certain sectoral agencies, notably Hong Kong's Securities and Futures Commission (SFC), have continued to press forward on cybersecurity regulation for specific industries.

This chapter discusses recent data privacy and cybersecurity developments in Hong Kong from August 2017 to July 2018. It will also discuss the current data privacy regulatory framework in Hong Kong, and in particular the six DPPs and their implications for organisations, as well as specific data privacy issues such as direct marketing, issues relating to technological innovation, international data transfer, cybersecurity and data breaches.

II THE YEAR IN REVIEW

i Personal data privacy and security developments

From mid-2015 to mid-2016, the PCPD issued a number of guidance notes, guidelines and codes of practice to assist organisations in implementing PDPO provisions. Notable publications included the October 2015 Guidance on Data Breach Handling and the Giving of Breach Notifications,[2] the April 2016 Revised Code of Practice on Human Resource

1 Yuet Ming Tham is a partner at Sidley Austin LLP.

2 www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf.

Management,[3] the April 2016 Privacy Guidelines: Monitoring and Personal Data Privacy at Work[4] and the June 2016 guidance note on Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users.[5] None of these publications are legally binding, although failure to follow the codes of practice may give rise to negative presumptions in any enforcement proceedings.

From mid-2016 to mid-2017, the PCPD did not issue any additional codes of practice or guidelines, but did release three revisions to existing guidance notes:

a Guidance on Data Breach Handling and the Giving of Breach Notifications (revised December 2016) (providing assistance to data users in handling breaches and mitigating loss and damage);[6]

b Guidance on CCTV Surveillance and Use of Drones (revised March 2017) (setting out recommendations on whether and how to use CCTV to properly protect data privacy);[7] and

c Proper Handling of Data Correction Request by Data Users (revised May 2017) (providing a step-by-step approach on the proper handling of a data correction request under the PDPO).[8]

From mid-2017 to mid-2018, the PCPD issued a new guidance note in December 2017 entitled Guidance on Election Activities for Candidates, Government Departments, Public Opinion Research Organisations and Members of the Public.[9] Additionally, the PCPD released revised Guidance on CCTV Surveillance and Use of Drones.[10]

The PCPD reported that it had received 3,501 complaints in 2017, which included 1,968 complaints relating to the reported loss of laptops by the Registration and Electoral Office containing personal data of election committee members and electors (the REO Incident). Excluding those complaints, the remaining 1,533 complaints represents a 17 per cent decrease from the 1,838 complaints received in 2016.[11] Most of the complaints involved were made against private sector organisations, with financial, property management, and telecommunications companies leading the way. Forty-one per cent of the complaints related to use of personal data without consent with about one-third complaining about the purpose and manner of the data collection. The PCPD received 237 ICT-related privacy complaints in 2017, representing a 3 per cent increase as compared to 2016. Most of these complaints related to the use of mobile apps and social networking websites. The PCPD received notice of 106 data breach incidents affecting 3.87 million persons in 2017 compared to 89 incidents involving 104,000 individuals the year before; however, taking out the REO Incident

3 www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/PCPD_HR_Booklet_Eng_AW07_Web.pdf.

4 www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf.

5 www.pcpd.org.hk/english/resources_centre/publications/files/DAR_e.pdf.

6 www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf (The publication on the PCPD website has not yet been updated).

7 www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf.

8 www.pcpd.org.hk/english/resources_centre/publications/files/dcr_e.pdf.

9 www.pcpd.org.hk/english/resources_centre/publications/files/electioneering_en.pdf.

10 www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf.

11 www.pcpd.org.hk/english/news_events/media_statements/press_20180214.html.

(which affected 3.78 million people), the number of affected individuals was only 86,000, representing a decrease of 17 per cent as compared to 2016. Direct marketing complaints decreased substantially in 2017, falling from 393 to 186 cases.

With respect to enforcement in 2017, the PCPD issued 26 warnings and three enforcement notices as compared to 36 warnings and six enforcement notices in 2016. Referrals to the police of cases for criminal prosecutions fell substantially compared to 2016, from 112 to 19, almost all of which involved direct marketing violations. The number of actual prosecutions remained relatively flat (four prosecutions in 2017 compared to five in 2016). All four prosecutions in 2017 resulted in convictions. One was for a company director who failed to comply with a summons issued by the Privacy Commissioner, and the other three concerned direct marketing violations. In January 2018, PARKnSHOP pled guilty to using the personal data of a data subject in direct marketing without obtaining the data subject's consent, resulting in a HK$3,000 fine.[12]

The PCPD does not systematically publish decisions or reports based on the outcome of its investigations. For the entirety of 2017 and up until June 2018, the PCPD published one investigation report[13] in 2017 (offering recommendations to estate agencies in ensuring compliance with the requirements under the PDPO).

ii Cybercrime and cybersecurity developments

Hong Kong does not have (and as of this writing, there do not appear to be plans to establish) stand-alone cybercrime and cybersecurity legislation. The Hong Kong Police Department maintains a resource page for 'Cybersecurity and Technology Crime', including a compendium of relevant legislation on computer crimes.[14] These specific provisions relate to the Crimes Ordinance, the Telecommunications Ordinance and laws related to obscenity and child pornography. The government has also established an Information Security (InfoSec) website that sets out various computer crime provisions contained in the Telecommunications Ordinance, the Theft Ordinance and the Crimes Ordinance.[15] According to the Hong Kong police, there were 5,939 computer crime cases in 2016, with an associated loss of HK$2.3 billion as compared to 6,862 cases in 2015 amounting to a loss of HK$1.8 billion.[16] (Figures were not available for 2017 as of the time of writing.)

Sectoral regulators have continued to press forward with specific cybersecurity regulation, particularly financial regulators. Both the SFC and the Hong Kong Monetary Authority (HKMA) have issued circulars on cybersecurity risk, and in May 2017, the SFC issued its Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading,[17] as well as a circular alert on ransomware threats in the securities

12 www.pcpd.org.hk/english/news_events/media_statements/press_20180102b.html.

13 www.pcpd.org.hk/english/enforcement/commissioners_findings/inspection_reports/files/R17-2201_Eng.pdf.

14 www.police.gov.hk/ppp_en/04_crime_matters/tcd/legislation.html.

15 www.infosec.gov.hk/english/ordinances/corresponding.html.

16 www.infosec.gov.hk/english/crime/statistics.html.

17 www.sfc.hk/edistributionWeb/gateway/EN/consultation/doc?refNo=17CP4.

industry.[18] In December 2016, the HKMA announced implementation details of its Cybersecurity Fortification Initiative undertaken in collaboration with the banking industry[19] as well as launching an industry-wide Enhanced Competency Framework on Cybersecurity.[20]

iii 2018 developments and regulatory compliance

From a regulatory perspective, the key compliance framework for companies and organisations remains with data protection and privacy. The government has not taken any additional legislative steps in the cybercrime and cybersecurity arenas although cybersecurity remains a significant challenge in Hong Kong. Financial sector regulators continue to be active with respect to cybersecurity, with the HKMA putting forward ambitious initiatives. For companies outside the financial sector, their focus will remain with PDPO compliance, particularly with the stringent direct marketing requirements.

III REGULATORY FRAMEWORK

i The PDPO and the six DPPs

The PDPO entered into force on 20 December 1996 and was amended by the Personal Data (Privacy) (Amendment) Ordinance 2012 (Amendment Ordinance). The majority of the provisions of the Amendment Ordinance entered into force on 1 October 2012 and the provisions relating to direct marketing and legal assistance entered into force on 1 April 2013.

The PCPD has issued various codes of practice and guidelines to provide organisations with practical guidance to comply with the provisions of the PDPO. Although the codes of practice and guidelines are only issued as examples of best practice and organisations are not obliged to follow them, in deciding whether an organisation is in breach of the PDPO, the PCPD will take into account various factors, including whether the organisation has complied with the codes of practice and guidelines published by the PCPD. In particular, failure to abide by certain mandatory provisions of the codes of practice will weigh unfavourably against the organisation concerned in any case that comes before the Privacy Commissioner. In addition, a court is entitled to take that fact into account when deciding whether there has been a contravention of the PDPO.

As mentioned above, the six DPPs of the PDPO set out the basic requirements with which data users must comply in the handling of personal data. Most of the enforcement notices served by the PCPD relate to contraventions of the six DPPs. Although a contravention of the DPPs does not constitute an offence, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

DPP1 – purpose and manner of collection of personal data

Principle

DPP1 provides that personal data shall only be collected if it is necessary for a lawful purpose directly related to the function or activity of the data user. Further, the data collected must be adequate but not excessive in relation to that purpose.

18 www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC26.

19 www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf.

20 www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf.

Data users are required to take all practicable steps to ensure that on or before the collection of the data subjects' personal data (or on or before first use of the data in respect of item (d) below), the data subjects were informed of the following matters:

a the purpose of collection;

b the classes of transferees of the data;

c whether it is obligatory to provide the data, and if so, the consequences of failing to supply the data; and

d the right to request access to and request the correction of the data, and the contact details of the individual who is to handle such requests.

Implications for organisations

A personal information collection statement (PICS) (or its equivalent) is a statement given by a data user for the purpose of complying with the above notification requirements. It is crucial that organisations provide a PICS to their customers before collecting their personal data. On 29 July 2013, the PCPD published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their PICS. It is recommended that the statement in the PICS explaining what the purpose of the collection is should not be too vague and too wide in scope, and the language and presentation of the PICS should be user-friendly. Further, if there is more than one form for collection of personal data each serving a different purpose, the PICS used for each form should be tailored to the particular purpose.

DPP2 – accuracy and duration of retention

Principle

Under DPP2, data users must ensure that the personal data they hold are accurate and up to date, and are not kept longer than necessary for the fulfilment of the purpose.

After the Amendment Ordinance came into force, it is provided under DPP2 that if a data user engages a data processor, whether within or outside Hong Kong, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than necessary for processing the data. 'Data processor' is defined to mean a person who processes personal data on behalf of a data user and does not process the data for its own purposes.

It should be noted that under Section 26 of the PDPO, a data user must take all practicable steps to erase personal data held when the data are no longer required for the purpose for which they were used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased. Contravention of this Section is an offence, and offenders are liable for a fine.

Implications for organisations

The PCPD published the Guidance on Personal Data Erasure and Anonymisation (revised in April 2014), which provides advice on when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and physical destruction. For example, it is recommended that dedicated software, such as that conforming to industry standards (e.g., US Department of Defense deletion standards), be used to permanently delete data on various types of storage devices. Organisations are also advised to adopt a top-down approach in respect of data destruction, and this requires the development

of organisation-wide policies, guidelines and procedures. Apart from data destruction, the guidance note also provides that the data can be anonymised to the extent that it is no longer practicable to identify an individual directly or indirectly. In such cases, the data would no longer be considered as 'personal data' under the PDPO. Nevertheless, it is recommended that data users must still conduct a regular review to confirm whether the anonymised data can be re-identified and to take appropriate action to protect the personal data.

DPP3 – use of personal data

Principle

DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. 'Prescribed consent' means express consent given voluntarily and that has not been withdrawn by notice in writing.

Implications for organisations

Organisations should only use, process or transfer their customers' personal data in accordance with the purpose and scope set out in their PICS. If the proposed use is likely to fall outside the customers' reasonable expectation, organisations should obtain express consent from their customers before using their personal data for a new purpose.

DPP4 – data security requirements

Principle

DPP4 provides that data users must use all practicable steps to ensure that personal data held are protected against unauthorised or accidental processing, erasure, loss or use.

After the Amendment Ordinance came into force, it is provided under DPP4 that if a data user engages a data processor (such as a third-party IT provider to process personal data of employees or customers), whether within or outside Hong Kong, the data users must adopt contractual or other protections to ensure the security of the data. This is important, because under Section 65(2) of the PDPO, the data user is liable for any act done or practice engaged in by its data processor.

Implications for organisations

In view of the increased use of third-party data centres and the growth of IT outsourcing, the PCPD issued an information leaflet entitled 'Outsourcing the Processing of Personal Data to Data Processors', in September 2012. According to this leaflet, it is recommended that data users incorporate contractual clauses in their service contracts with data processors to impose obligations on them to protect the personal data transferred to them. Other protection measures include selecting reputable data processors, and conducting audits or inspections of the data processors.

The PCPD also issued the Guidance on the Use of Portable Storage Devices (revised in July 2014), which helps organisations to manage the security risks associated with the use of portable storage devices. Portable storage devices include USB flash cards, tablets or notebook computers, mobile phones, smartphones, portable hard drives and DVDs. Given that large amounts of personal data can be quickly and easily copied to such devices, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policies and practice. The guidance note recommended that a risk assessment be carried out to guide the development of an organisation-wide policy to manage the risk

associated with the use of portable storage devices. Further, given the rapid development of technology, it is recommended that this policy be updated and audited regularly. Some technical controls recommended by the guidance note include encryption of the personal data stored on the personal storage devices, and adopting systems that detect and block the saving of sensitive information to external storage devices.

DPP5 – privacy policies

Principle

DPP5 provides that data users must publicly disclose the kind of personal data held by them, the main purposes for holding the data, and their policies and practices on how they handle the data.

Implications for organisations

A privacy policy statement (PPS) (or its equivalent) is a general statement about a data user's privacy policies for the purpose of complying with DPP5. Although the PDPO is silent on the format and presentation of a PPS, it is good practice for organisations to have a written policy to effectively communicate their data management policy and practice. The PCPD published a guidance note entitled Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement, which serves as guidance for data users when preparing their PPS. In particular, it is recommended that the PPS should be in a user-friendly language and presentation. Further, if the PPS is complex and lengthy, the data user may consider using proper headings and adopting a layered approach in presentation.

DPP6 – data access and correction

Principle

Under DPP6, a data subject is entitled to ascertain whether a data user holds any of his or her personal data, and to request a copy of the personal data. The data subject is also entitled to request the correction of his or her personal data if the data is inaccurate.

Data users are required to respond to a data access or correction request within a statutory period of 40 days. If the data user does not hold the requested data, it must still inform the requestor that it does not hold the data within 40 days.

Implications for organisations

Given that a substantial number of disputes under the PDPO relate to data access requests, the PCPD published a guidance note entitled Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users, dated June 2012, to address the relevant issues relating to requests for data access. For example, although a data user may impose a fee for complying with a data access request, a data user is only allowed to charge the requestor for the costs that are 'directly related to and necessary for' complying with a data access request. It is recommended that a data user should provide a written explanation of the calculation of the fee to the requestor if the fee is substantial. Further, a data user should not charge a data subject for its costs in seeking legal advice in relation to the compliance with the data access request.

ii Direct marketing

Hong Kong's regulation of direct marketing deserves special attention from organisations engaging in such activities. Unlike with violations of the DPPs, violations of the PDPO's direct marketing provisions are criminal offences, punishable by fines and by imprisonment. The PCPD has demonstrated a willingness to bring enforcement actions in this area and to refer particularly egregious violations for criminal prosecution.

Revised direct marketing provisions under the PDPO

The revised direct marketing provisions under the Amendment Ordinance entered into effect on 1 April 2013, and introduced a stricter regime that regulates the collection and use of personal data for sale and for direct marketing purposes.

Under the revised direct marketing provisions, data users must obtain the data subjects' express consent before they use or transfer the data subjects' personal data for direct marketing purposes. Organisations must provide a response channel (e.g., email, online facility or a specific address to collect written responses) to the data subject through which the data subjects may communicate their consent to the intended use. Transfer of personal data to another party (including the organisation's subsidiaries or affiliates) for direct marketing purposes, whether for gain or not, will require express written consent from the data subjects.

Guidance on Direct Marketing

The PCPD published the New Guidance on Direct Marketing in January 2013 to assist businesses to comply with the requirements of the revised direct marketing provisions of the PDPO.

Direct marketing to corporations

Under the New Guidance on Direct Marketing, the Privacy Commissioner stated that in clear-cut cases where the personal data are collected from individuals in their business or employee capacities, and the product or service is clearly meant for the exclusive use of the corporation, the Commissioner will take the view that it would not be appropriate to enforce the direct marketing provisions.

The Privacy Commissioner will consider the following factors in determining whether the direct marketing provisions will be enforced:

a the circumstances under which the personal data are collected: for example, whether the personal data concerned are collected in the individual's business or personal capacity;

b the nature of the products or services: namely, whether they are for use of the corporation or for personal use; and

c whether the marketing effort is targeted at the business or the individual.

Amount of personal data collected

While the Privacy Commissioner has expressed that the name and contact information of a customer should be sufficient for the purpose of direct marketing, it is provided in the New Guidance on Direct Marketing that additional personal data may be collected for direct marketing purposes (e.g., customer profiling and segmentation) if the customer elects to supply the data on a voluntary basis. Accordingly, if an organisation intends to collect additional personal data from its customers for direct marketing purposes, it must inform

its customers that the supply of any other personal data to allow it to carry out specific purposes, such as customer profiling and segmentation, is entirely voluntary, and obtain written consent from its customers for such use.

Penalties for non-compliance

Non-compliance with the direct marketing provisions of the PDPO is an offence, and the highest penalties are a fine of HK$1 million and imprisonment for five years.

Spam messages

Direct marketing activities in the form of electronic communications (other than person-to-person telemarketing calls) are regulated by the Unsolicited Electronic Messages Ordinance (UEMO). Under the UEMO, businesses must not send commercial electronic messages to any telephone or fax number registered in the do-not-call registers. This includes text messages sent via SMS, pre-recorded phone messages, faxes and emails. Contravention of the UEMO may result in fines ranging from HK$100,000 to HK$1 million and up to five years' imprisonment.

In early 2014, the Office of the Communications Authority prosecuted a travel agency for sending commercial facsimile messages to telephone numbers registered in the do-not-call registers. This is the first prosecution since the UEMO came into force in 2007. The case was heard before a magistrate's court, but the defendant was not convicted because of a lack of evidence.

Person-to-person telemarketing calls

Although the Privacy Commissioner has previously proposed to set up a territory-wide do-not-call register on person-to-person telemarketing calls, this has not been pursued by the government in the recent amendment of the PDPO.[21] Nevertheless, under the new direct marketing provisions of the PDPO, organisations must ensure that they do not use the personal data of customers or potential customers to make telemarketing calls without their consent. Organisations should also check that the names of the customers who have opted out from the telemarketing calls are not retained in their call lists.

On 5 August 2014, the Privacy Commissioner issued a media brief to urge the government administration to amend the UEMO to expand the do-not-call registers to include person-to-person calls. In support of the amendment, the Privacy Commissioner conducted a public opinion survey, which revealed that there had been a growing incidence of person-to-person calls, with more people responding negatively to the calls and fewer people reporting any gains from the calls. Although there had been long-standing discussions regarding the regulation of person-to-person calls in the past, it remains to be seen whether any changes will be made to the legislation.

Enforcement

Following prosecution referrals by the PCPD, Hong Kong courts handed down the first penalties in direct marketing violations in 2015. In September 2015, the Hong Kong Magistrates' Court convicted the Hong Kong Broadband Network Limited (HKBN) for violating the PDPO's requirement that a data user cease using an individual's personal data in

21 Report on Further Public Discussions on Review of the Personal Data (Privacy) Ordinance (April 2011).

direct marketing upon request by that individual.[22] The court imposed a fine of HK$30,000. In a separate court action from September 2015, Links International Relocation Limited pleaded guilty to a PDPO direct marketing violation for not providing required information to a consumer before using his personal data in direct marketing.[23] The court fined the company HK$10,000.

Additional convictions and fines followed in 2015 and 2016 for direct marketing violations. The most recent cases initiated by the PCPD resulting in fines and convictions were a January 2017 guilty plea by DBS Bank for failing to comply with a customer request to cease using personal data in direct marketing, resulting in a HK$10,000 fine,[24] and a December 2016 guilty plea from a watch company that failed to obtain consent and to inform the consumer of his rights under the PDPO before engaging in direct marketing to the consumer, resulting in a HK$16,000 fine.[25] Given the large number of criminal referrals by the PCPD with respect to direct marketing violations, we expect direct marketing prosecutions to continue to be an active enforcement area.

iii Technological innovation and privacy law

Cookies, online tracking and behavioural advertising

While there are no specific requirements in Hong Kong regarding the use of cookies, online tracking or behavioural advertising, organisations that deploy online tracking that involves the collection of personal data of website users must observe the requirements under the PDPO, including the six DPPs.

The PCPD published an information leaflet entitled 'Online Behavioural Tracking' (revised in April 2014), which provides the recommended practice for organisations that deploy online tracking on their websites. In particular, organisations are recommended to inform users what types of information are being tracked by them, whether any third party is tracking their behavioural information and to offer users a way to opt out of the tracking.

In cases where cookies are used to collect behavioural information, it is recommended that organisations preset a reasonable expiry date for the cookies, encrypt the contents of the cookies whenever appropriate, and do not deploy techniques that ignore browser settings on cookies unless they can offer an option to website users to disable or reject the cookies.

The PCPD also published the Guidance for Data Users on the Collection and Use of Personal Data through the Internet (revised in April 2014), which advises organisations on compliance with the PDPO while engaging in the collection, display or transmission of personal data through the internet.

Cloud computing

The PCPD published the information leaflet 'Cloud Computing' in November 2012, which provides advice to organisations on the factors they should consider before engaging in cloud computing. For example, organisations should consider whether the cloud provider

22 www.pcpd.org.hk/english/news_events/media_statements/press_20150909.html. HKBN appealed, and in 2017, the Hong Kong High Court dismissed the appeal, confirming that HKBN's communication was for the purpose of direct marketing. See www.onc.hk/en_US/can-data-user-received-data-subjects-opt-request-continue-promote-services-part-sale-service.

23 www.pcpd.org.hk/english/news_events/media_statements/press_20150914.html.

24 www.pcpd.org.hk/english/news_events/media_statements/press_20170110.html.

25 www.pcpd.org.hk/english/news_events/media_statements/press_20161206.html.

has subcontracting arrangements with other contractors, and what measures are in place to ensure compliance with the PDPO by these subcontractors and their employees. In addition, when dealing with cloud providers that offer only standard services and contracts, the data user must evaluate whether the services and contracts meet all security and personal data privacy protection standards they require.

On 30 July 2015, the PCPD published the revised information leaflet 'Cloud Computing' to advise cloud users on privacy, the importance of fully assessing the benefits and risks of cloud services and the implications for safeguarding personal data privacy. The new leaflet includes advice to organisations on what types of assurances or support they should obtain from cloud service providers to protect the personal data entrusted to them.

Employee monitoring

In April 2016, the PCPD published the revised Privacy Guidelines: Monitoring and Personal Data Privacy at Work, to aid employers in understanding steps they can take to assess the appropriateness of employee monitoring for their business, and how they can develop privacy-compliant practices in the management of personal data obtained from employee monitoring. The guidelines are applicable to employee monitoring activities whereby personal data of employees are collected in recorded form using the following means: telephone, email, internet and video.

Employers must ensure that they do not contravene the DPPs of the PDPO while monitoring employees' activities. The PDPO has provided some additional guidelines on monitoring employees' activities and has recommended employers to do the following:

a Evaluate the need for employee monitoring and its impact upon personal data privacy. Employers are recommended to undertake a systematic three-step assessment process:
- 'assessment' of the risks that employee monitoring is intended to manage and weigh that against the benefits to be gained;
- 'alternatives' to employee monitoring and other options available to the employer that may be equally cost-effective and practical but less intrusive on an employee's privacy; and
- 'accountability' of the employer who is monitoring employees, and whether the employer is accountable and liable for failure to be compliant with the PDPO in the monitoring and collection of personal data of employees.

b Monitor personal data obtained from employee monitoring. In designing monitoring policies and data management procedures, employers are recommended to adopt a three-step systematic process:
- 'clarify' in the development and implementation of employee monitoring policies the purposes of the employee monitoring; the circumstances in which the employee monitoring may take place; and the purpose for which the personal data obtained from monitoring records may be used;
- 'communication' with employees to disclose to them the nature of, and reasons for, the employee monitoring prior to implementing the employee monitoring; and
- 'control' over the retention, processing and the use of employee monitoring data to protect the employees' personal data.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Section 33 of the PDPO deals with the transfer of data outside Hong Kong, and it prohibits all transfers of personal data to a place outside Hong Kong except in specified circumstances, such as where the data protection laws of the foreign country are similar to the PDPO or the data subject has consented to the transfer in writing. Section 33 of the PDPO has not been brought into force since its enactment in 1995, and although implementation has been consistently discussed in recent years, the government currently has no timetable for its implementation.

V COMPANY POLICIES AND PRACTICES

Organisations that handle personal data are required to provide their PPS to the public in an easily accessible manner. In addition, prior to collecting personal data from individuals, organisations must provide a PICS setting out, *inter alia*, the purpose of collecting the personal data and the classes of transferees of the data. As mentioned above, the PCPD has published the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement (see Section III.i), which provides guidance for organisations when preparing their PPS and PICS.

The Privacy Management Programme: A Best Practice Guide (see Section II.i) also provides guidance for organisations to develop their own privacy policies and practices. In particular, it is recommended that organisations should appoint a data protection officer to oversee the organisation's compliance with the PDPO. In terms of company policies, apart from the PPS and PICS, the Best Practice Guide recommends that organisations develop key policies on the following areas: accuracy and retention of personal data; security of personal data; and access to and correction of personal data.

The Best Practice Guide also emphasises the importance of ongoing oversight and review of the organisation's privacy policies and practices to ensure they remain effective and up to date.

VI DISCOVERY AND DISCLOSURE

i Discovery

The use of personal data in connection with any legal proceedings in Hong Kong is exempted from the requirements of DPP3, which requires organisations to obtain prescribed consent from individuals before using their personal data for a new purpose (see Section III.i). Accordingly, the parties in legal proceedings are not required to obtain consent from the individuals concerned before disclosing documents containing their personal data for discovery purposes during legal proceedings.

ii Disclosure

Regulatory bodies in Hong Kong, such as the Hong Kong Police Force, the Independent Commission Against Corruption and the Securities and Futures Commission, are obliged to comply with the requirements of the PDPO during their investigations. For example, regulatory bodies in Hong Kong are required to provide a PICS to the individuals prior to collecting information or documents containing their personal data during investigations.

Nevertheless, in certain circumstances, organisations and regulatory bodies are not required to comply with DPP3 to obtain prescribed consent from the individuals concerned. This includes cases where the personal data are to be used for the prevention or detection of crime, and the apprehension, prosecution or detention of offenders, and where compliance with DPP3 would be likely to prejudice the aforesaid purposes.

Another exemption from DPP3 is where the personal data is required by or authorised under any enactment, rule of law or court order in Hong Kong. For example, the Securities and Futures Commission may issue a notice to an organisation under the Securities and Futures Ordinance requesting the organisation to produce certain documents that contain its customers' personal data. In such a case, the disclosure of the personal data by the organisation would be exempted from DPP3 because it is authorised under the Securities and Futures Ordinance.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Public enforcement

An individual may make a complaint to the PCPD about an act or practice of a data user relating to his or her personal data. If the PCPD has reasonable grounds to believe that a data user may have breached the PDPO, the PCPD must investigate the relevant data user. As mentioned above, although a contravention of the DPPs does not constitute an offence in itself, the PCPD may serve an enforcement notice on data users for contravention of the DPPs, and a data user who contravenes an enforcement notice commits an offence.

Prior to the amendment of the PDPO in 2012, the PCPD was only empowered to issue an enforcement notice where, following an investigation, it is of the opinion that a data user is contravening or is likely to continue contravening the PDPO. Accordingly, in previous cases where the contraventions had ceased and the data users had given the PCPD written undertakings to remedy the contravention and to ensure that the contravention would not continue or recur, the PCPD could not serve an enforcement notice on them as continued or repeated contraventions were unlikely.

Since the entry into force of the Amendment Ordinance, the PCPD has been empowered to issue an enforcement notice where a data user is contravening, or has contravened, the PDPO, regardless of whether the contravention has ceased or is likely to be repeated. The enforcement notice served by the PCPD may direct the data user to remedy and prevent any recurrence of the contraventions. A data user who contravenes an enforcement notice commits an offence and is liable on first conviction for a fine of up to HK$50,000 and two years' imprisonment and, in the case of a continuing offence, a penalty of HK$1,000 for each day on which the offence continues. On second or subsequent conviction, the data user would be liable for a fine of up to HK$100,000 and imprisonment for two years, with a daily penalty of HK$2,000.

ii Private enforcement

Section 66 of the PDPO provides for civil compensation. Individuals who suffer loss as a result of a data user's use of their personal data in contravention of the PDPO are entitled to compensation by that data user. It is a defence for data users to show that they took reasonable steps to avoid such a breach.

After the Amendment Ordinance came into force, affected individuals seeking compensation under Section 66 of the PDPO may apply to the Privacy Commissioner for

assistance and the Privacy Commissioner has discretion whether to approve it. Assistance by the Privacy Commissioner may include giving advice, arranging assistance by a qualified lawyer, arranging legal representation or other forms of assistance that the Privacy Commissioner may consider appropriate.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Although the PDPO does not confer extraterritorial application, it applies to foreign organisations to the extent that the foreign organisations have offices or operations in Hong Kong. For example, if a foreign company has a subsidiary in Hong Kong, the Hong Kong subsidiary will be responsible for the personal data that it controls, and it must ensure the personal data are handled in accordance with the PDPO no matter whether the data are transferred back to the foreign parent company for processing.

IX CYBERSECURITY AND DATA BREACHES

i Cybercrime and cybersecurity

As previously noted, Hong Kong does not have stand-alone cybercrime or cybersecurity legislation. The Computer Crimes Ordinance, which was enacted nearly 25 years ago in 1993, amended the Telecommunications Ordinance,[26] the Crimes Ordinance[27] and the Theft Ordinance,[28] expanding the scope of existing criminal offences to include computer-related criminal offences. These include:

a unauthorised access to any computer; damage or misuse of property (computer program or data);

b making false entries in banks' books of accounts by electronic means;

c obtaining access to a computer with the intent to commit an offence or with dishonest intent; and

d unlawfully altering, adding or erasing the function or records of a computer.

Although Hong Kong does not currently have cybersecurity legislation, the government does support a number of organisations dedicated to responding to cyber threats and incidents. These entities include the Hong Kong Emergency Response Team Coordination Centre (managed by the Hong Kong Productivity Council) for coordinating responses for local enterprises and internet users, and the Government Computer Emergency Response Team Hong Kong (a work unit established under the Office of the Government Chief Information Officer), which is a team charged with coordinating and handling incidents relating to both the private and public sectors. In addition, the Hong Kong Police Force has established the Cyber Security and Technology Crime Bureau, which is responsible for handling cybersecurity issues and combating computer crime.

26 Sections 24 and 27 of the Telecommunications Ordinance.

27 Sections 59, 60, 85 and 161 of the Crimes Ordinance.

28 Sections 11 and 19 of the Theft Ordinance.

ii Data breaches

There is currently no mandatory data breach notification requirement in Hong Kong. In October 2015 and then again in December 2016, the PCPD revised its Guidance on Data Breach Handling and the Giving of Breach Notifications, which provides data users with practical steps in handling data breaches and to mitigate the loss and damage caused to the individuals involved. Although the PCPD noted in the Guidance that there are no statutory notification requirements, the PCPD recommended that data users strongly consider notifying affected persons and relevant authorities, such as the PCPD. In particular, after assessing the situation and the impact of the data breach, the data users should consider whether the following persons should be notified as soon as practicable:

a the affected data subjects;
b the law enforcement agencies;
c the Privacy Commissioner (a data breach notification form is available on the PCPD's website);
d any relevant regulators; or
e other parties who may be able to take remedial actions to protect the personal data privacy and the interests of the data subjects affected (e.g., internet companies such as Google and Yahoo! may assist in removing the relevant cached link from their search engines).

X OUTLOOK

Hong Kong's data privacy and protection framework is long-standing and relatively mature. We expect that the PCPD will continue enforcement at generally the same levels, with continued emphasis on direct marketing violations and prosecution referrals for such violations.

In recent public statements, the PCPD has emphasised the importance of striking a balance between privacy protection and free flow of information, engaging small- and medium-sized businesses in promoting the protection of and respect for personal privacy, and strengthening the PCPD's working relationship with mainland China and overseas data protection authorities. We expect that the PCPD and the Hong Kong government will continue to emphasise the development of Hong Kong as Asia's premier data hub and to provide additional policy, promotional and incentive support to facilitate growth in the region.

With respect to cybercrime and cybersecurity, we do not anticipate major legislation in the near term and expect that sectoral regulators will continue to take the lead in these areas.

Appendix 1

ABOUT THE AUTHORS

YUET MING THAM

Sidley Austin LLP

Yuet is a global head of the government litigation and investigations group, and head of the Asia-Pacific compliance and investigations group. Besides compliance and investigations, Yuet focuses on privacy and cybersecurity work. She speaks fluent English, Mandarin, Cantonese and Malay and is admitted in New York, England and Wales, Hong Kong, and Singapore.

Yuet was most recently awarded the Emerging Markets 'compliance and investigations lawyer of the year' by *The Asian/American Lawyer*, with the team also recognised as the 'compliance/investigations firm of the year'. She has also been acknowledged as a 'leading lawyer' by *Chambers Asia-Pacific* across four categories namely 'dispute resolution: litigation,' 'corporate investigations/anti-corruption,' 'life sciences' and 'financial services: contentious regulatory.' Additionally, Yuet is recognised in the 'financial services regulatory' in *IFLR1000* as a 'leading lawyer' and has also been listed by *Who's Who Legal* as a 'leading business lawyer' in 'life sciences,' 'business crime defense' and 'investigations.' In the 2018 edition of *Chambers Asia-Pacific*, Yuet is described as 'exceptionally bright' and 'very responsive and knowledgeable and can immediately dive into the issues'. The 2015 edition of *Chambers Global* stated 'Ms Tham is described by clients as "a marvellous and gifted attorney"'. Meanwhile, *Chambers Asia-Pacific* noted that Yuet 'is frequently sought after by international corporations, who respect her experience and expertise in risk management'.

SIDLEY AUSTIN LLP

39/F Two International Finance Centre
Central
Hong Kong
Tel: +852 2509 7645
Fax: +852 2509 3110

Level 31, Six Battery Road
Singapore 049909
Tel: +65 6230 3969
Fax: +65 6230 3939

yuetming.tham@sidley.com
www.sidley.com

ISBN 978-1-912228-62-1