Panel on Constitutional Affairs

Review of the Personal Data (Privacy) Ordinance and related matters

Major issues raised at the special meeting on 20 November 2010

I. Powers of the Privacy Commissioner for Personal Data
(Proposals 7, 39, 40 and 42 in the Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance ("the consultation report"))

The Administration proposes to confer the Privacy Commissioner for Personal Data ("PCPD") with the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under section 66 of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"). The Administration, however, does not propose to grant criminal investigation and prosecution power to PCPD, to empower PCPD to award compensation to aggrieved data subjects, or to impose monetary penalty on serious contravention of Data Protection Principles ("DPPs").

Deputations' views	**PCPD's views**	**Members' views**
Granting criminal investigation and prosecution power to PCPD	Granting criminal investigation and prosecution power to PCPD	Granting criminal investigation and prosecution power to PCPD
Some deputations have urged the Administration to grant criminal investigation and prosecution power to PCPD but a deputation takes the view that PCPD should not be conferred with the power to carry out criminal investigations and prosecutions as it is important to retain the existing arrangement under which the criminal investigation and prosecution are undertaken respectively by the Police and Department of Justice in order to maintain checks and balances.	Granting criminal investigation and prosecution power to PCPD will help avoid criticism of favouritism where the Police or other government departments are involved in the case as data user. The discretion whether or not to prosecute shall remain reserved for the Secretary for Justice and the	Some members have expressed support for granting criminal investigation and prosecution power to PCPD in order to enhance personal data privacy protection. While some members have expressed support for

Deputations' views	PCPD's views	Members' views
	power to judge the culpability of any data user stays with the Judiciary.	strengthening the powers of PCPD including his powers to conduct investigations, they consider that vesting enforcement, criminal investigation and prosecution powers in a single body is against the principle of natural justice and may lead to inadequate checks and balances.
Empowering PCPD to award compensation to aggrieved data subjects	Empowering PCPD to award compensation to aggrieved data subjects	
Two individuals have expressed the view that empowering PCPD to award compensation to aggrieved data subjects is the most efficient mechanism to address their damages. It has been suggested that if the proposal to empower PCPD to award compensation to data subjects is not pursued, the two privacy civil torts (i.e. the tort of intrusion upon another's solitude or seclusion and the tort of unwarranted publicity) proposed by the Law Reform Commission should be enacted to allow data subjects to seek damages for unfair collection and unfair release of personal data.	The power will have direct deterrent effect against infringement of PDPO and should be granted to PCPD in order to provide remedy to the aggrieved data subjects without the need to go through legal process.	

Deputations' views	**PCPD's views**	**Members' views**
Empowering PCPD to impose monetary penalty on serious contravention of DPPs	Empowering PCPD to impose monetary penalty on serious contravention of DPPs	
	The proposal will greatly enhance the power of PCPD to penalize data users for blatant disregard of personal data privacy rights.	
Provision of legal assistance	Provision of legal assistance	Provision of legal assistance
Some deputations have expressed support for the proposal of empowering PCPD to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation under section 66 of PDPO. It is considered that before legal action is resorted, PCPD should seek to mediate the complaint and the claim for compensation. Another deputation, however, considers that PCPD should provide guidance and advice instead of legal assistance to an aggrieved data subject as the legal aid system is well-established in Hong Kong.	As there is no express provision under PDPO for PCPD to carry out mediation of a complaint, an additional power should be conferred on PCPD to carry out mediation of a complaint including settlement by a monetary sum.	A member has expressed support that PCPD should be empowered to provide legal assistance to an aggrieved data subject to institute legal proceedings to seek compensation and further suggested that a fund similar to the Consumer Legal Action Fund should be set up to give aggrieved data subjects greater access to legal remedies by providing financial support and legal assistance. She also agrees that PCPD should be given the power to mediate complaints.

Deputations' views	**PCPD's views**	**Members' views**
Others	Others	
An individual has suggested that PCPD should be empowered under section 43 of PDPO to conduct public hearing for cases of great public concern. An individual has expressed concern that PCPD does not have adequate power to search and seize evidence which will hamper his investigation work. A deputation has suggested that a statutory obligation should be imposed on government organizations and pubic bodies to provide professional/technical assistance to PCPD in order to strengthen his investigation power.	Flexibility should be introduced to allow PCPD to decide whether a hearing should be conducted in public having regard to all circumstances. Power to search and seize evidence as well as power to call upon public officers for assistance should be granted to PCPD.	

II. "Opt-in" mechanism versus "opt-out" mechanism
(Proposals 1 and 2 in the consultation report)

The Administration proposes to require the data user, on or before collecting personal data, to provide an option for the applicant to choose not to agree to ("opt-out" mechanism) the use (including transfer) of his/her personal data for any of the intended direct marketing activities or the transfer of the data to any class of transferees. The Administration considers it not appropriate to introduce a territory-wide "Do-not-call" register against direct marketing activities. For the sale of personal data, the Administration invites public views on whether the data subject should be provided with an opportunity to indicate his/her agreement to ("opt-in" mechanism) or his/her disagreement with ("opt-out" mechanism) the sale.

Deputations' views	**PCPD's views**	**Members' views**
Deputations from the direct marketing/exhibition and convention industries strongly support the adoption of an "opt-out" mechanism for the collection and use of personal data on the grounds that (a) adopting an "opt-in" mechanism would seriously affect the business of the relevant industries resulting in abundant job loss; (b) there is no country where an "opt-in" mechanism has been adopted across the board; (c) person-to-person telemarketing conducted directly by data users are generally accepted by the general public; and (d) only basic business contacts with no sensitive personal information will be collected at exhibitions and trade fairs. Objection has been expressed to the requirement for a data user to specify at the time of collection the direct marketing activities for which the personal data collected are to be used in view of the changing market situation. These deputations have suggested that - (a) more specific requirements should be added to ensure transparency and full disclosure of information to allow consumers to opt out; and	Introducing an "opt-in" mechanism is consistent with the overwhelming public expectation for greater self-determination and can ensure that the data subject's preference is made known directly and without doubt. PCPD has made the following suggestions - (a) a central "Do-not-call" register should be set up to deal with person-to-person telemarketing calls involving personal data which can be set up as an independent register run by office of PCPD or incorporated in the Office of the Telecommunications Authority's Do-not-call register. (b) an obligation should be imposed on a direct marketer to disclose the source of the personal data upon the data	A member has expressed support for adopting an "opt-out" mechanism on the grounds that it has been adopted by most western countries and the Administration has already proposed to introduce additional specific requirements to strengthen the regulation over the collection and use of personal data in direct marketing as well as sale of personal data. While expressing support for an "opt-out" mechanism to facilitate business developments, some members considers that data users should have the obligation to stipulate clear provisions for data subjects to indicate their choice. Another member, however, is of the view that adopting an "opt-out" mechanism does not afford adequate safeguards to the

Deputations' views	PCPD's views	Members' views
(b) a "tick-box" should be provided to make it as easy as possible for consumers to opt out and consumers should be given another opportunity to opt out if new use of the personal data is contemplated. Some other deputations are of the view that an "opt-in" mechanism should be adopted for direct marketing activities for better protection of personal data. They consider that the relevant industries should come up with proposals to ensure better protection of the personal data of consumers when advocating the adoption of an "opt-out" mechanism. In addition, there can be different modes to implement the "opt-in" mechanism which does not have to be applied across-the-board. These deputations urge PCPD to compile the Register of Data Users as soon as possible and have suggested that - (a) a territory-wide "Do-not-call" register for person-to-person telemarketing should be established; and (b) PCPD should be granted the power to stipulate the scopes of personal data which can be collected from data subjects in specific trades and business sectors.	subject's request in order to facilitate the data subject to trace the culpable ones on suspected contravention of PDPO.	personal data privacy as explicit consent of consumer is not required.

Deputations' views	**PCPD's views**	**Members' views**
Two individuals have made the following suggestions - (a) if an "opt-out" mechanism is adopted, data subjects should be offered an opt-out option specific to each of the direct marketing purposes of the personal data collected; (b) a central "Do-not-call" register for person-to-person telemarketing should be established; and (c) in addition to the right to be informed of the sources of their personal data, data subjects should have the right to retain control over their personal data such as the right to know about transfer destinations of their personal data, the right to correct or delete their personal data.		

III. Personal data security breach notification
(Proposal 6 in the consultation report)

The Administration proposes to start with the adoption of a voluntary notification system, with guidance notes issued by PCPD to assist data users in handling data breaches and to facilitate them in giving data breach notifications.

Deputations' views	PCPD's views	Members' views
Some deputations are of the view that a mandatory personal data security breach notification system should be introduced in phases. The following suggestions have been made - (a) the mandatory system should apply to government organizations/public bodies and a voluntary system to the private sector; (b) a mandatory system can be applied initially to high-risk private business sectors such as the finance and banking sector which involve frequent use of personal data, and the application can be further extended to other business sectors having regard to the level of sensitivity of personal data involved and the degree of the impact arising from any leakage; and (c) PCPD should be notified of cases where there is serious potential damage arising from leaked personal data such as disclosure of financial and medical data with personal identifiers so that PCPD will be in the best position to access the risks and decide whether notifications should be issued to the affected data subjects, and it should be mandatory for the data users to notify the affected data subjects in cases when there is chance	A mandatory data breach notification should be introduced in phases.	

Deputations' views	PCPD's views	Members' views
of leakage of personal data and potential damage of data subjects is also expected.		

IV. Sensitive personal data
(Proposal 38 in the consultation report)

The Administration does not propose to institute a statutory regulatory regime for sensitive personal data at this stage. The Administration proposes that PCPD should step up promotion and education and where necessary, issue a code of practice or guidelines to suggest good practices on the handling and use of sensitive data in general, such as biometric data and health records; and PCPD should continue to discuss with the information technology sector possible measures to enhance the protection of biometric data.

Deputations' views	PCPD's views	Members' views
Some deputations are of the view that the Administration should introduce a categorization system for sensitive personal data with a view to applying different degrees of regulation according to the categorization. When enhancing the regulation, the Administration should draw up clear guidelines for the information technology industry to follow. It has been suggested that classes of sensitive data should be defined in legislation for additional protection as follows :	There should be a more stringent regulation of sensitive personal data. Protection level of special categories of personal data should be brought at par with the standard stipulated in the European Union Directive 95/46/EC. Article 8 of the Directive provides that "*Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs,*	

Deputations' views	PCPD's views	Members' views
- authentication/identification data (e.g. biometric features); - reputational data (e.g. HIV status); - group membership that could be discriminated against (e.g. homosexuality/ ethnic origins); and - location of people for the protection against spousal abuse or stalking.	*trade-union membership, and the processing of data concerning health or sex life*."	

V. Implementation of section 33 of PDPO

The Administration proposes to make more preparation work before bringing the provision into operation.

Deputations' views	PCPD's views	Members' views
Most deputations have expressed support for the implementation of section 33 of PDPO, but a deputation has expressed concern that its implementation might affect the operation of the exhibition and convention industry as transfer of data to overseas countries is a frequent and common practice in the industry.	PCPD has completed the preparatory work for the implementation of section 33 of PDPO and is ready to implement the provision, pending the Administration's decision.	A member considers that section 33 of PDPO should be brought into operation as soon as practicable. Some other members, however, are of the view that as PDPO was enacted in 1995, a re-assessment of its impact on industries concerned may be warranted in view of the technological advancement and

Deputations' views	PCPD's views	Members' views
		prevalence of cross-boundary business operations in recent years.

Council Business Division 2
Legislative Council Secretariat
16 December 2010