Speech delivered by Mr. Allan Chiang,  
Privacy Commissioner for Personal Data  
at ONC Conference on Law Reform  
“Does Law Reform need Reforming in Hong Kong?”  
on 17 September 2011 at Rayson Huang Theatre,  
The University of Hong Kong  

Reviewing the Personal Data (Privacy) Ordinance  
through Standstill and Crisis

Protection of privacy interests

Privacy is an all-embracing concept which covers the following interests:

(a) the interest of the person in controlling the information held by others about him, or “information privacy” (or “informational self-determination” as it is referred to in Europe);  
(b) the interest in controlling entry to the “personal place”, or “territorial privacy”;  
(c) the interest in freedom from interference with one’s physical person, or “personal privacy”; and  
(d) the interest in freedom from surveillance and from interception of one’s communications, or “communications and surveillance privacy”.

Various sources of privacy law afford protection of these interests. First, articles 28, 29 and 30 of the Basic Law provide constitutional protection to personal privacy, territorial privacy and communications privacy respectively. In addition, Article 17 of the International Covenant of Civil and Political Rights (“ICCPR”) (incorporated in Article 14 of the Hong Kong Bill of Rights Ordinance) provides for a guarantee against arbitrary or unlawful interference with privacy. The ICCPR also imposes on the Government an obligation to adopt legislative and other measures to give effect to the prohibition against interference with the right to privacy. In this regard, a series of reports were issued by the Law Reform Commission (“LRC”) recommending that

---

1 Note: This paper depicted the state of affairs as at 13 July 2011 when the Personal Data (Privacy) (Amendment) Bill 2011 was introduced into the Legislative Council.  
legislation be introduced to better protect these privacy interests. They comprise:

(a) Reform of the Law Relating to the Protection of Personal Data (August 1994),
(b) Privacy: Regulating the Interception of Communications (December 1996),
(c) Stalking (October 2000),
(d) Civil Liability for Invasion of Privacy (December 2004),
(e) Privacy and Media Intrusion (December 2004), and
(f) Privacy: The Regulation of Covert Surveillance (March 2006).

Of these, only the recommendations of the first two and the last LRC reports were duly taken up by the Government and implemented. In particular, the Personal Data (Privacy) Ordinance ("PDPO") came into effect in December 1996. It is worth exploring why and how legislation on personal data protection received a priority treatment.

*Personal Data (Privacy) Bill: getting off the ground*

The first clue can be found in the statement of purpose put forward by the Government when it introduced the Personal Data (Privacy) Bill into the Legislative Council ("LegCo") on 19 April 1995, namely[^3],

(i) to protect the privacy interests of individuals in relation to personal data, and
(ii) to safeguard the free flow of personal data to Hong Kong from the imposition of restrictions by the increasing number of countries that already have data protection laws.

Clearly, the first point provides a generic reason while the second point explains the real driver for the change. As Berthold and Wacks suggest[^4], the Government at that time perceived a risk that Hong Kong’s trade position could be jeopardized if legislation on data privacy was not in place. Specifically, the concerns related to adoption of the EU Directive on Privacy[^5] by the European

Parliament in 1995, the year that the Hong Kong Bill was introduced. Article 25(1) of the EU Directive provides that member states shall provide that the transfer to a third country of personal data that are undergoing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection. As the directive is binding on the United Kingdom among other European countries, it seems natural for the British government to take up the incumbency to introduce relevant data protection legislation in Hong Kong for the purpose of safeguarding the continued free flow of cross-border data. There was urgency in the process as the sovereignty of Hong Kong was to be returned to China in two years’ time.

The Government’s concerns were vehemently supported by members of the LegCo upon the second reading of the Bill on 27 July 1995:

“Advanced countries of the world have already legislated to protect personal data. To ensure that Hong Kong can continue to exchange information, especially electronic data, with these countries, including Hong Kong’s most important trading partners, Hong Kong must have in place corresponding legislations [sic], which are of utmost important in maintaining and developing Hong Kong as the international centre for communication of the Asia-Pacific region. The community has already come to a very clear political and policy understanding in this regard.”

“… I could say that the Administration would like to (have) this Bill passed into law as soon as possible because the Administration knows clearly that if by 1996 we still do not have such legal protection in place, the exchange of trade and commercial information would be greatly affected, especially when the European Union has already passed a resolution in this regard.”

On the same day, the Bill was read the third time and passed with amendments. Looking back, the Bills Committee, set up only on 16 May 1995 to study the Bill, completed its mission in about two months’ time. This miraculous act led to the enactment of the PDPO on 3 August 1995. The core provisions of the

of such Data”,

6 Legislative Council Secretariat (1995) Legislative Council Meeting on 27 July 1995, p 6192,
7 Ibid. p 6194.
Ordinance came into effect on 20 December 1996, shortly before the handover of the sovereignty of Hong Kong from Britain to China.

**Legislative proposals to protect other privacy interests in limbo**

On the other hand, the other three LRC reports on privacy interests are still in limbo. In reply to a question raised at the Legislative Council on 10 November 2010, the Government responded as follows:-

“... As regards the LRC’s Report on Civil Liability for Invasion of Privacy and Report on Privacy and Media Intrusion, there were mixed responses and divergent views in the community. The proposed recommendations of the two reports were highly contentious and involved a number of complicated legal concepts (for example, the definitions of “reasonable expectation of privacy” and “unwarranted publicity given to the private life of another person”). When deciding the way forward, we need to reach a consensus in the community and strike a balance between different rights such as rights to personal privacy and freedom of the press.

Among the LRC reports on privacy, the report on “stalking” is comparatively less controversial. Hence, we will first deal with that report. The report proposed the introduction of legislation in order to render the pursuit of a course of conduct causing another person alarm or distress a criminal offence and a civil wrong. We are examining the report and will cautiously consider those proposals which may impact on press freedom. We are also examining latest developments on overseas legislation such as how they regulate collective harassment. As an important step to follow up on the LRC report, we will make practical preparation for conducting public consultation in the coming few months. We plan to launch a consultation exercise in mid-2011....”

The hypothesis

While the Government’s intention to protect privacy interests generally is not disputed, the history outlined above seems to indicate that the real impetuses

---

for introducing new legislation are events or even crises outside the control of Government, rather than a proactive lead from the Government.

Judging from the Government’s response or non-response to the proposed legislation for personal and territorial privacy, it would appear that the Government’s priorities in law reform are very much influenced by how controversial the subject matter is. Priorities would be devoted to less controversial subjects because in these cases, it would be easier to reach a consensus in the community and strike a balance between privacy rights and other conflicting rights.

This hypothesis can be further tested in tracing the developments in the review of PDPO leading to the introduction of the Personal Data (Privacy) (Amendment) Bill in July 2011.

**Review of PDPO**

The PDPO is a robust piece of legislation in personal data protection.\(^9\) It covers any data relating directly or indirectly to a living individual ("data subject") from which it is practicable to ascertain directly or indirectly the identity of the individual and which are in a form in which access or processing is practicable. It applies to any person ("data user") who controls the collection, holding, processing or use of personal data. Data users must follow the six Data Protection Principles ("DPPs") in Schedule 1 to PDPO in relation to the purpose and manner of data collection, accuracy and duration of data retention, use of personal data, security of personal data, transparency of data protection policies and practices, and access to and correction of personal data.

PDPO is in line with international privacy standards as the six DPPs are broadly consistent with the 1980 OECD Guidelines\(^{10}\). It is even stronger in some important aspects, having incorporated some of the requirements of the 1995 EU Directive. However, in light of operating experience in an evolving privacy landscape, the need for amendments to the PDPO was quickly felt soon after it became effective.

---


Since 1998, the Office of the Privacy Commissioner for Personal Data (“PCPD”) had submitted proposals for piecemeal legislative amendments to the Home Affairs Bureau (the Hong Kong SAR Government’s policy bureau responsible for human rights and access to information at that time) for the Government’s consideration. The proposals were largely technical in nature aimed at addressing the practical issues identified in relation to the implementation of the PDPO. The Bureau had given green light to some of the proposals and had in fact given Draft Drafting Instructions to the Law Drafting Division of the Department of Justice in preparing an Amendment Bill. The first draft of the Amendment Bill was prepared in 2002 but was subsequently stalled.

Renewed strength pushing for legislative changes was gained in recent years when Hong Kong witnessed a series of privacy catastrophes gaining widespread media attention. In March 2006, a serious data leakage incident broke out involving disclosure on the internet of the personal data of some 20,000 people who had lodged complaints with the Independent Police Complaints Council (“IPCC”) against the Police. The data concerned included names, addresses, Hong Kong ID card numbers and in some cases details of criminal convictions. Their leakage, caused by IPCC’s contractor for computing services, immediately posed an alarming threat to the persons affected. PCPD conducted an investigation\(^\text{11}\) and found that IPCC had contravened DPP4 of Schedule 1 to PDPO for failing to take all reasonably practicable steps to ensure that personal data held by it are protected against unauthorized or accidental access, processing, erasure or other use. An enforcement notice was issued to IPCC directing it to take various remedial measures, including the formulation and implementation of policy, guidelines and measures to protect the complaint data when dealing with an outsourced contractor. As the PCPD found that IPCC had complied fully with the enforcement notice, no prosecution was initiated.

In the subsequent two to three years, more incidents of data leakage or loss broke out\(^\text{12}\), involving large quantities of personal data held by major data users.


These include:-

(a) loss of portable storage devices containing patient records by a number of public hospitals, exemplified by the loss reported by the Prince of Wales Hospital on 6 May 2008 of a USB flash drive containing 10,000 patients’ personal data;
(b) in July 2007, the personal particulars of 13,400 taxpayers were recorded by an officer of the Inland Revenue Department for his future personal use;
(c) from May 2008 to February 2009, classified and sensitive documents containing personal data held by the Immigration, Police and Fire Services Departments were leaked on the internet through the file-sharing software called “Foxy”;
(d) incidents that took place in the commercial sector, including the leakage from the recruitment website Recruit.net of the personal data of 40,000 online job seekers in June 2007 and the loss by the Hongkong and Shanghai Banking Corporation of a computer server containing 159,000 customers in April 2008.

This spate of data breaches had attracted a lot of media attention and created much public debate about the role of the PCPD and the adequacy of the PDPO in protecting personal data.

Against this background, it was no coincidence that the PCPD took the initiative in June 2006 to form an internal working group to conduct a comprehensive review of the PDPO with a view to identifying necessary amendments to ensure it is still current and relevant in safeguarding personal data. Its proactive efforts culminated in a formal submission in December 2007 of various amendment proposals to the Government’s Constitutional and Mainland Affairs Bureau (“CMAB”, the policy bureau which took over from the Home Affairs Bureau the responsibility for human rights since July 2007). The subject was discussed at the meeting of the LegCo’s Panel on Home Affairs on 4 July 2008. Members of the Panel expressed overwhelming support for enhanced protection of personal data privacy and that the Government should study the amendment proposals seriously. Upon request for a timetable for the Government to complete an evaluation of the amendment proposals, CMAB responded that “... it aimed at coming up with concrete
proposals to amend PDPO for consultation with the Fourth Term LegCo as early as possible”.

Areas of concern in implementing PDPO

The major data breach incidents that took place since the implementation of the PDPO have highlighted a number of areas of concern.

It was generally felt that the existing provisions of the PDPO are inadequate in safeguarding personal data protection. In the event of data leakage, data users are not mandated to notify the affected persons. Further, PCPD does not have adequate sanctioning power to ensure compliance with the PDPO. It has no specific function to mediate between the parties concerned to reach a mutually satisfactory settlement. It has no authority to award compensation to aggrieved data subjects or to impose monetary penalties on data users for contraventions of the DPPs. The aggrieved data subject is left on his own to institute legal proceedings against the data user concerned to seek compensation under PDPO. Such civil action claims have rarely been brought before the court by the aggrieved data subject. This is understandable due to the high litigation costs relative to the amount of damages to be awarded in normal circumstances and that there is no guarantee that the claimant may remain anonymous throughout the legal proceedings.

In fact, contravention of the DPPs is not an offence per se. The most forceful action PCPD may take is to issue an enforcement notice to direct the data user to take specified remedial steps within a specified period. Only if the data user contravenes the enforcement notice will he commit an offence. The punitive effect of this arrangement is weak. The PCPD may serve an enforcement notice only when a contravention is likely to continue or be repeated. Further, in the event that a data user resumes the same contravening act shortly after compliance with the enforcement notice, the PCPD can only issue another enforcement notice. This represents a loophole for data users to circumvent PCPD’s escalation of regulation from issue of enforcement notice to prosecution of an offence.

Where prosecution of an offence is contemplated for contravention of the requirements under the PDPO, including breach of an enforcement notice, the PCPD is not empowered to institute prosecutions directly against the data users
concerned. Instead, the PCPD has to refer suspected offences to the Police for criminal investigation and where deemed necessary, to the Department of Justice for prosecution. In this aspect PCPD’s enforcement powers are clearly wanting.

The amendment proposals and public consultation

One year after its formal pledge at LegCo, CMAB completed a review of the PDPO in conjunction with PCPD and published on 28 August 2009 a consultation document inviting views from the public on or before 30 November 2009 on a series of proposed amendments to the PDPO.\(^\text{14}\) By way of background introduction, it recognized in the document the following developments which prompted the need to review whether the existing provisions of the PDPO are still adequate for protecting personal data:-

(a) the challenges posed by the rapid advancement in information technology, prevalence of the Internet and exponential growth of e-commerce;
(b) the operational and technical issues identified since the implementation of the PDPO; and
(c) the community’s increasing concern about personal data privacy protection.

CMAB made it clear in the document that the review was guided by the following factors: \(^\text{15}\)

(a) the right of individuals to privacy is not absolute. It must be balanced against other rights and public and social interests;
(b) balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology;
(c) any changes to the privacy law should not undermine Hong Kong’s competitiveness and economic efficiency as an international city;
(d) the need to avoid putting onerous burden on business operations and individual data users;
(e) due account should be given to local situations;

\(^{14}\) HKSAR Government, *Consultation Document on Review of the Personal Data (Privacy) Ordinance* (Aug 2009),

\(^{15}\) Ibid, p iii, para 4.
(f) the PDPO should remain flexible and relevant in spite of technological change;

(g) legislative intervention may not always be the most effective way. In certain circumstances, personal data privacy protection may be achieved by administrative measures; and

(h) consensus in the community about the privacy issues is important.

While the starting point is the protection of personal data privacy, the emphasis on protecting business interests and arriving at a community consensus is very strong and it will be apparent in the analysis below that these are the main factors determining whether a proposal will be followed up by the Government.

In the consultation document, CMAB put forward what it coined as 12 “key proposals” as follows:-

(a) **Sensitive personal data**
   Personal data commonly regarded as sensitive by overseas jurisdictions include racial or ethnic origin, political opinion, religious or philosophical beliefs, membership of trade union, health condition, sexual life, criminal record and biometric information. At present, the PDPO does not differentiate personal data that are sensitive from those that are not. Given the gravity of harm that may be inflicted upon the data subject in the event of leakage or accidental disclosure to third parties of sensitive personal data, the issue is whether the processing of sensitive personal data should be subject to more stringent data protection requirements to better protect the personal data privacy of individuals. A more stringent regulatory regime, such as prohibiting the collection, holding, processing and use of such data, is in line with international practices and standards.

(b) **Regulation of data processors and sub-contracting activities**
   The rising trend of data users sub-contracting and entrusting data processing work to third parties has increased the risk to which personal data may be exposed. At present, the PDPO regulates data users but not their agents. In the event of a data breach committed by the agent, the protection afforded to the data subjects is for the data user to assume liability as the principal. The issue is whether to directly regulate the data processors or to indirectly regulate them by requiring the data user to use contractual or other means to ensure its agents observe the requirements under the PDPO as regards use,
security and safekeeping of the personal data entrusted to them, or a combination of these two options.

(c) **Personal Data Security Breach Notification**
At present, there is no requirement under the PDPO for a data user to notify a personal data breach to the PCPD or individuals affected by the breach. The issue is whether such a notification system should be instituted, on a mandatory or voluntary basis, so that the affected data subjects may take steps to protect themselves or to mitigate the harm that could be done to them.

(d) **Granting criminal investigation and prosecution power to the PCPD**
At present, the PDPO confers powers on the PCPD to investigate into suspected breaches of the PDPO’s requirements and to inspect personal data systems for promoting compliance with the PDPO. These powers include entry into premises, summoning witnesses and requiring such persons to furnish relevant information, but exclude search for or seizure of evidence. Criminal investigations are conducted by the Police and prosecutions, where necessary, are initiated by the Department of Justice. The issue is whether PCPD should be given the criminal investigation and prosecution power, as well as the incidental powers to search and seize evidence with a view to achieving more effective enforcement of the PDPO.

(e) **Legal assistance to data subjects**
At present, a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user is entitled to compensation from the data user for that damage. However, as the aggrieved party has to bear the legal costs, such recourse to civil remedy under the PDPO is rarely invoked. The issue is whether PCPD should be empowered to offer legal assistance to the data subject to seek redress with a view to achieving greater deterrent effect on acts or practices which intrude into personal data privacy.

(f) **Award compensation to aggrieved data subjects**
As noted above, an aggrieved data subject may under the PDPO seek compensation from the data user for the damage he has suffered by reason of the data user’s contravention of a requirement under the PDPO. However, the court proceedings involved could be lengthy and costly, and the
outcome is unpredictable. The issue is whether, as a quick and additional means of redress, the PCPD should be empowered to determine and award compensation to the aggrieved data subject.

(g) **Imposing monetary penalty on serious contravention of DPPs**

The issue is whether to empower the PCPD to require data users to pay monetary penalty for serious contravention of DPPs, in order to produce a greater deterrent effect.

(h) **Making contravention of a DPP an offence**

The PCPD is empowered to remedy a contravention of a DPP by issuing an enforcement notice to the data user concerned. Contravention of the enforcement notice is an offence but contravention of the DPPs *per se* is not. The issue is whether to make the contravention of a DPP an offence in order to achieve a greater deterrent effect.

(i) **Unauthorized obtaining, disclosure and sale of personal data**

Unauthorized use of personal data may intrude into personal data privacy and cause serious harm to data subjects. These may include intentional or wilful acts such as unauthorized access and collection of customers’ personal data by the staff of a company for sale to third parties for profit, and malicious disclosure of a patient’s sensitive health records by hospital staff to third parties. The issue is whether to make these blatant acts an offence.

(j) **Repeated contravention of a DPP on same facts**

At present, a data user may, shortly after compliance with an enforcement notice issued against him within a specified period, resume the same contravening act without fear of a criminal sanction. This is because the PCPD in the circumstances can only issue yet another enforcement notice. The issue is whether to make such a repeated contravention an offence in order to forestall possible circumvention of the regulatory regime.

(k) **Repeated non-compliance with enforcement notice**

At present, the PDPO does not differentiate, in terms of severity of sanctions, between the first contravention of an enforcement notice and repeated contraventions. The issue is whether to subject a repeated offender to heavier penalty in order to achieve a greater deterrent effect.
(l) Raising penalty for misuse of personal data in direct marketing

Under section 34 of the PDPO, a data user shall not use any personal data for direct marketing activities if the data subject has made an opt-out request. Otherwise he commits an offence and is liable to a fine at Level 3 (up to $10,000). In view of the prevalence of direct marketing activities in Hong Kong and that many unsolicited telemarketing calls are causing nuisance to many people, the PCPD is of the view that the existing level of penalty may be too low to serve as an effective deterrent. The issue is whether the penalty level for a section 34 offence should be raised.

In addition, the consultation document includes 31 proposals on which public comments were also invited. They cover the following areas:

(a) the rights of data subjects under the PDPO;
(b) the rights and obligations of data users under the PDPO;
(c) enforcement powers of the PCPD;
(d) exemptions from the requirements of the PDPO; and
(e) streamlining the operation of the PDPO and addressing the technical and operational problems encountered in the implementation of the PDPO.

Under (c), one proposal is to provide the PCPD with wider discretion to serve an enforcement notice. At present, the PCPD may serve an enforcement notice on a data user if the latter is contravening a requirement under the PDPO or has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated. To enhance the effectiveness of the PDPO, it was proposed to allow the PCPD to serve an enforcement notice even if the contravening act has ceased and there is no likelihood of repetition, provided that the act involved has caused or is likely to cause damage or distress to the data subject.

Furthermore, the consultation document includes a number of proposals made by the PCPD but not favoured by the Government. Of these, two proposals on revamping the regulatory regime of direct marketing are worth noting here:

(a) “Opt-in”

Apart from raising the penalty level for a section 34 offence, the proposal requires the data user to obtain the explicit consent of the data subject (that
is, “opt-in”) before using the latter’s personal data from any source for direct marketing purposes. This recognizes the data subject’s right of self-determination on his personal data, as opposed to the alternative of “opt-out” which places the burden on the data subject to indicate his wish not to be approached by direct marketers.

(b) Central Do-not-call register

The PCPD recognizes that under the Unsolicited Electronic Messages Ordinance (“UEMO”), OFTA is already operating a “Do-not-call” register prohibiting the sending of commercial electronic messages to any telephone or fax number registered. The PCPD proposes therefore that OFTA’s “Do-not-call” register should be expanded to include person-to-person telemarketing calls. Under this proposal, consumers may “opt-out” by registering their personal data (i.e. names and telephone numbers) in a central “Do-not-call” register operated by the Government. Telemarketers making calls to selected consumers would need to check this register beforehand and it would be an offence for them to make unsolicited calls to registered consumers against their opt-out wish.

As noted in the consultation document, CMAB planned to set the general directions on the way forward based on the views gathered from the consultation exercise, and “arrange for further public discussions on possible legislative proposals” ¹⁶ (emphasis added). There was no promise that the exercise will definitely lead to legislative amendments. However, when CMAB released its report ¹⁷ on the public consultation on 18 October 2010, the prospects for legislative amendments were more definite. As noted in the report, the Government has formulated general directions on the way forward and shall arrange to further collect public views and meet with relevant organisations or stakeholders for “in-depth discussions on the details of the proposals planned to be taken forward, including the contents of the legislative amendments, so as to ensure smooth operation of the amended PDPO” ¹⁸ (emphasis added). The process of “further public discussions” ended on 31 December 2010 and a report ¹⁹ was released on 18 April 2011 from which it is noted that “in the light of the views received, (the Administration)

¹⁶ Supra n 14, p iv, para 5.
¹⁸ Ibid, Ch 1, p 3, para 1.8.
has revised and refined the details of some of the proposals and will implement the proposals …… (the Administration is) **preparing a bill to amend the PDPO** to implement these proposals. (Its) aim is to introduce it into the LegCo in July 2011” 20 (emphasis added). As it turned out, the Personal Data (Privacy) (Amendment) Bill 2011 (“the Bill”) was introduced into the LegCo on 13 July 2011.

Looking back, it took less than two years for the Government to prepare the Bill, counting from the release of the first public consultation document. By any yardstick, this is an impressive record. It is postulated that the main driver for this accelerating pace of change was a major privacy intrusion incident that took place in 2010 committed by the Octopus group of companies.

**The Octopus Incident**

The Octopus incident was a landmark privacy intrusion event which concerned the misuse of customer data held by a group of companies which operate a smartcard payment system called Octopus. The Octopus card is widely used by the man in the street for day to day needs. It almost obviates the need for change in the daily lives of the Hong Kong people.

Octopus’s majority shareholder is the Mass Transit Railway Corporation (“MTR”). In turn, the majority shareholder of MTR is the Hong Kong SAR Government.

Capitalising on its huge customer database, Octopus collaborated with its business partners to deliver direct marketing and customer loyalty programmes. In particular, it operates a customer reward programme whereby registered members could earn Reward Dollars for making purchases from Octopus’ business partners by presenting the Octopus card. The Reward Dollars earned may be redeemed for goods and services from these business partners.

Since March 2010, subscribers for the programme started to complain about Octopus’ transfer of their personal data to third parties for direct marketing purposes without their knowledge or consent. The PCPD investigated into the complaints and found, among other things, the following contraventions:-

---

20 Ibid, Ch 5, p 42, para 5.2.
(a) First, the notice informing the customers of the purpose of the use of the personal data collected, and the classes of persons to whom the data would be transferred, was poorly laid out and presented. For example, the font size used for the notice was so small (about 1mm x 1mm for English) that people with normal eyesight would find the words difficult to read unless aided by a magnifying glass.

(b) Secondly, the purpose of use of personal data and classes of data transferees were couched in liberal and vague terms. It would not be practicable for customers to ascertain with a reasonable degree of certainty how their personal data could be used and who could have the use of them.

(c) Thirdly, Octopus had, without the customers’ explicit consent, transferred their personal data to a number of partner companies for marketing the latter’s products and services. Octopus played little or no part in the marketing process. But it received monetary gains from the partner companies as a reward for the data transfer. The transaction in essence was a sale of personal data.

(d) Finally, under prior agreement with Octopus, one partner company promoted its products and services by calling Octopus’ customers in the name of Octopus. In effect, the customers have been deceived as regards the identity of the caller.

The Octopus incident attracted prolonged media attention and strong protests from different interest groups in Hong Kong. It was rated as one of the top ten news stories of 2010 by many newspapers in Hong Kong. It is indeed a major milestone in the history of personal data protection in Hong Kong, characterized by a number of unique features:-

(a) It represented the tip of an iceberg as similar misuse of customers’ personal data was not uncommon in business enterprises such as banks with a large customer database.

---

(b) It involved the handling of personal data of 2.4 million people, one-third of the entire population of Hong Kong, for substantial monetary gain.
(c) Octopus is a household name which all Hong Kong citizens have a high regard for. When they found out that their personal data had been traded like a commodity for the private gain of Octopus, it was no surprise that they reacted with a sense of betrayal and fury.

The effects on Octopus for its outright failure to observe privacy and data protection were detrimental. The loss of public trust and damage to its corporate image are probably irreparable. The public outcry did not subside until it had taken a series of drastic remedial actions as follows:-

(a) It accepted all the recommendations of the PCPD and those of other regulators as regards enhancing personal data protection.
(b) It donated to charity all the revenue generated by its data transfer to third parties, viz. HK$57.9 m.
(c) It pledged that it would focus its core business on providing smart card services to customers and it would no longer participate in activities that require the provision of customer data to merchant partners for marketing purposes.
(d) Both its CEO and Board chairman resigned (the latter purportedly as part of a natural succession plan).

It is perhaps no exaggeration to say that the Octopus incident provided a human rights lesson for the Hong Kong community. It raised public awareness and understanding of their privacy rights over personal data to an unprecedentedly high level. Media reports on privacy and data protection issues are more prevalent than ever before. In a subsequent survey conducted by an internet security company from February to March 2011, it was found that 85% of Hong Kong people surveyed were extremely or very concerned about misuse of their personal data.22

---

The Octopus incident had important implications for the corporate data users too. It served as a wake-up call to those who might not have accorded adequate priority to the issue of personal data privacy. Transfer of customers’ personal data to third parties for direct marketing purposes is pretty common in Hong Kong. The trades involved include the banks, the telecommunication operators and the insurance industries. The corresponding trade regulators for these trades were under great pressure to address the issues raised by Octopus’ malpractice. For example, the Hong Kong Monetary Authority, which oversees the banks, went as far as to direct the banks to suspend the transfer of personal data to unrelated third parties for marketing purposes unless and until they were able to confirm full compliance with the law and the Guidance Note issued by the PCPD.

As the ownership of Octopus can be traced to the Government, the incident generated immense political interests and fuelled vicious attacks against the Government for maladministration. Legislators blamed the Secretary for Transport and the Secretary for Financial Services, who sit on the MTR Board, for dereliction of duties and held them accountable for Octopus’ contraventions. Both Legislator Wong Kwok-hing and Legislator James To had proposed to invoke the Legislative Council (Powers and Privileges) Ordinance to investigate into the Octopus incident. The latter went even further to propose the appointment of a select committee under this Ordinance to inquire into issues relating to the transfer and sale of customers’ personal data in the banking sector, the telecommunications sector, the insurance sector and large-scale chain stores which had induced members of the public to provide them with personal data through various reward programmes.

Legislator Wong claimed victory for making MTR accept responsibility for the Octopus’ misdeed and take drastic remedial actions, and withdrew his proposal accordingly. He noted that the Chief Executive had made a special note in his policy address on 13 October 2010 that the Government would put forward legislative proposals to enhance personal data protection. He was reported to have said, “as the Administration was expected to complete the review (on

25 Ibid para 71.
26 Supra n 23, p 388.
PDPO) by the end of the year, he considered that the way forward should be to press the Administration to submit its legislative proposals to LegCo as soon as possible in early 2011.”  

Legislator To’s proposals were not supported after an intense debate and voting at the House Committee of the LegCo on 26 November 2010. It is worth noting that the debate made a great deal of reference to CMAB’s concurrent effort in reviewing the PDPO. There seems to be a consensus among the Committee members that the existing legislation is inadequate in protecting personal data privacy. They noted that PCPD was not even able under the PDPO to serve an enforcement notice on Octopus because the evidence showed the contraventions would not continue or be repeated. Among other things, Legislator To stressed that his proposed cross-industry inquiry would compel the organizations concerned to produce all relevant information regarding transfer and sale of customers’ personal data and this would serve as a factual basis for LegCo to consider the Government’s proposals for amending the PDPO. On the other hand, many other Committee members present shared the views of Legislator Wong that given the Government had initiated a review of the PDPO, it would be more fruitful for them to focus on the review and to be more vigilant in the scrutiny of the legislative proposals in future.

In short, there is no question that the Government was put on the spot to expedite the required legislative amendment process to enhance personal data protection. This probably provides the parties concerned the quickest escape from an embarrassing political turmoil.

**Further legislative proposals to regulate collection and use of personal data for direct marketing**

In the report on public consultation issued on 18 October 2010, CMAB specifically introduced further legislative proposals to address the urgent need to strengthen regulation over the collection and use (including sale) of personal data for direct marketing. These included:

(a) introduction of additional specific requirements on the collection and use of personal data for direct marketing purposes, and to make it an offence if a

---

27 Supra n 24, para 63.
28 Supra n 24.
29 Supra n 17.
data user does not comply with the requirements and subsequently uses the personal data for direct marketing:

(i) requiring the data user’s notice to the data subject about data collection to be reasonably specific about the intended marketing activities, the classes of persons to whom the data may be transferred and the kinds of data to be transferred;
(ii) the presentation of the information should be understandable and reasonably readable; and
(iii) the data subject should be provided with an opportunity to opt out from the intended use of his/her personal data.

The offence attracts a maximum fine of HK$500,000 and imprisonment for three years.

(b) making unauthorized sale of personal data by data user an offence, punishable by a maximum fine of HK$1,000,000 and imprisonment for five years.

**Screening out legislative proposals**

It is interesting to explore how the Government decided to take forward a legislative proposal based on the views collected from the consultation exercises. As expected, the amendment proposals attracted diverse views from the public and they were duly recorded in the reports released on 18 October 2010 and 18 April 2011 respectively. CMAB attempted to adopt a qualitative and analytical approach in examining the public views and concluding on the way forward. By reading between the lines, however, one cannot help postulate that the screening process could well be a simple mathematical game:

(1) proposals that have the majority support (in terms of percentage of submissions arguing in favour) were taken forward;
(2) proposals with a majority arguing against were stalled; and
(3) proposals with no clear support or opposition were stalled as well.

Included in category (1) are the following proposals:-

(a) Personal Data Security Breach Notification (on voluntary basis)
(b) Legal assistance to data subjects
(c) Unauthorized obtaining, disclosure and sale of personal data
(d) Repeated non-compliance with enforcement notice
(e) Raising penalty for misuse of personal data in direct marketing
(f) Introduction of specific requirements on collection and use of personal data for direct marketing purpose
(g) Making unauthorized sale of personal data an offence.

Included in category (2) are the following proposals:-

(a) Granting criminal investigation and prosecution power to the PCPD
(b) Awarding compensation to aggrieved data subjects
(c) Imposing monetary penalty on serious contravention of DPPs
(d) Making contravention of a DPP an offence.

Included in category (3) are the following proposals:-

(a) Affording greater protection to sensitive personal data
(b) Regulation of data processors and sub-contracting activities
(c) Setting up a Central Do-not-call register.

There are three notable exceptions to the above simple mathematical approach to screening of legislative proposals. Firstly, as regards whether to make a repeated contravention of a DPP on same facts an offence, it was reported that there were mixed views of supporting and opposing the proposal, but no indication was mentioned as regards which side was outnumbered. The conclusion was that the Government would implement the proposal\(^{30}\).

Secondly, as regards whether to allow the PCPD to serve an enforcement notice even if the contravening act has ceased and there is no likelihood of repetition, it was reported that some 40% of the submissions opposed the implementation of the proposal while over 30% indicated their support. Despite the lack of a majority support, CMAB concluded to proceed with the proposal\(^{31}\). It is conceivable that this extraordinary decision was prompted by the inability of the PCPD to issue an enforcement notice in the Octopus case. This impotence was criticized by some media and legislators as setting the culprit free.

\(^{30}\) Supra n 17, pp 69-73.
\(^{31}\) Supra n 17, pp 52-54.
Thirdly, as regards the choice between an “opt-in” or an “opt-out” regime for seeking customers’ consent to use their personal data for direct marketing, the reports did not mention at all which option has more support from the public. Instead, the Government argued in favour of “opt-out” on grounds that it is less onerous to the operations of enterprises and it is more widely adopted in overseas jurisdictions.  

A simple mathematical approach counting the number of submissions for and against a proposal is beset with flaws. To begin with, the system appears to work on the basis of one submission equals one vote, with little or no weighting assigned based on the identity of the person making the submission and the arguments therein. Even PCPD’s submission, which represented the wisdom gained through years of experience of enforcing data protection in Hong Kong and well-grounded research based on worldwide trends and overseas experience, seems to attract only one plain vote.

Further, not to proceed with a proposal due to the lack of a clear majority support may be an overly restrictive approach. The words usually used in this regard in the consultation reports include “views … are evenly split”, “mixed views”, “no consensus could be reached” and “views … are diverse”. Bearing in mind that human rights issues including personal data protection are by nature controversial, the Government does not appear to be very enthusiastic in taking a proactive lead in promoting further public debates on the controversial issues and resolving them with the stakeholders concerned.

A case in point is PCPD’s proposal to accord greater protection to sensitive personal data by prohibiting the collection, holding, processing and use of such data except under prescribed circumstances. CMAB concluded on this proposal as follows:

“... most of the views support the general direction that a higher degree of protection should be afforded to certain types of personal data which are more sensitive. Nevertheless, views received are diverse with regard to the coverage of sensitive personal data with no mainstream consensus reached.... There are also quite a lot of views considering that the Government should consult the

---

32 Supra n 17, pp 8-13.
33 Supra n 17, pp 123-124.
public further before arriving at any conclusion... We shall keep in view the community’s discussion on whether sensitive personal data should be subject to more stringent regulation and the coverage of sensitive personal data, as well as the development and experience of overseas jurisdictions .... before we further consider whether to take forward the proposal .....”

Conclusion

The experience of the initial enactment of the PDPO and its impending amendment outlined above seems to indicate that the Government’s approach to legislative reform is reactive rather than proactive. The drive for change can be traced back to a perceived imminent risk to Hong Kong’s trade position in 1995 and a public outcry in 2010 underlining the inadequacy of the existing legislation. Without these impetuses, one wonders whether real progress would have been made.

This passive approach is explicable given the Government’s philosophy of pragmatic politics. The Chief Executive’s policy address34 made at the end of his previous term of office reveals the Government’s reluctance to “engage in ideological debates or utopian social projects”. In lieu of a moral pledge to promote human rights and consumer interests, the Chief Executive’s priorities are to “build a harmonious society” by “resolving conflicts” and “fostering consensus”.

At this stage of Hong Kong’s constitutional development, the Government lacks a strong direct mandate acquired through the electoral process, and is therefore prone to be a hostage to public opinion rather than a leader of public opinion. The current initiative to amend PDPO may be merely a passive reaction to the Octopus crisis, as evidenced by the emphasis on regulation of the direct marketing and sale of personal data, and the avoidance of issues with no consensus reached in the public consultations. We probably need further public outcries to prompt the Government to address seriously and expeditiously other and perhaps more controversial subjects in data protection and other privacy areas.