Review of the Personal Data (Privacy) Ordinance

Proposals to be Taken Forward

Submission by HKGCC

In the submission of the Hong Kong General Chamber of Commerce in response to the review of the Personal Data (Privacy) Ordinance (PDPO) in 2009, the importance of striking a balance between protecting personal data privacy and business efficacy was emphasised. As we review the "Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance" (the "report") published in October 2010, and the proposals the Government intends to take forward, we would like to once again highlight the importance of striking a balance.

Regulatory bodies tend to seek wider powers. But the Government needs to strike a right balance between protecting personal data privacy and business efficacy. None of us want to see the competitiveness of Hong Kong being compromised. Nor do we want to see the development of the ICT industry and business operations hindered if onerous burden and undue restrictions are imposed on business collection and usage of customer data.

While some public opinions might have swung to one side after recent customer data incidents involving some major companies, we would urge for caution when heavier penalties, such as criminalisation, is contemplated. Imposing criminal sanctions is no small matter as personal liberty is at stake. It is an overriding principle that any penalty should be proportionate to the prohibited conduct and its damage. We must avoid creating new criminal sanctions as a knee jerk reaction to controversial incidents, without first fully considering the justification.

The Chamber's detailed comments on the proposals to be taken forward are as follows:

Proposal (1): Collection and Use of Personal Data in Direct Marketing

Proposal (a)

The Chamber does not agree that the misuse of personal data in direct marketing under section 34 (1)(b)(ii) of the PDPO should attract criminal sanctions. In particular, imprisonment is a disproportionate penalty having regard to the nature of the conduct and the damage in most cases.

Both the consultation paper and the report on the consultation mentioned that considerations in determining the appropriate level of penalty should include whether the penalty can act as an effective deterrent, whether direct marketing activities bring serious damage to data subjects, and how penalty level would impact on economic activities.

As we argued in our last submission, while unsolicited marketing calls can be annoying, the actual material damage may not be substantial. While there are calls for raising the penalty, imposing imprisonment for conduct that merely creates annoyance without causing serious harm is disproportionate.

The economic value of direct marketing activities should not be overlooked. As noted in the Government's consultation paper issued in October 2009: "…direct marketing has its economic values with regard to provision of job opportunities and information on products and services available to consumers. An unduly heavy penalty for related offence may frustrate normal and legitimate marketing activities."

A survey commissioned by the Office of the Telecommunications Authority (OFTA) on person-to-person (P2P) calls[1] found that 21% of respondents indicating they agreed that P2P calls brought economic benefits to the community, and that 46% of respondents indicating that they would listen to the P2P calls to see whether they were interested. It is also important to note that the OFTA survey found that over half of P2P calls did not involve use of personal data, and that there was no overwhelming support for legislation to regulate P2P marketing calls.

We are of the view that OFTA's recommendations on P2P direct marketing calls strike a sensible balance between protecting consumer and ensuring business efficacy.

Proposal (b)

While we welcome the government's decision not to pursue Proposal (b), i.e. the "opt-in" proposal, we do not agree that customers should be provided with an additional option up-front for them to indicate that they do not agree to the use of their data for direct marketing. Section 34 of the PDPO already provides a mechanism for data subjects to opt-out upon first receiving direct marketing materials; this additional up-front option duplicates a well-established process that has been working reasonably well.

Even if customers are to be provided with an option, it would be clearly impractical to allow them to choose not to agree to the use of their data for any of the intended direct marketing activities or the transfer of the data to any class of transferees, as this will mean data users will have to provide a tailor-made opt-out process to cater for the specific requirements of each customer. This will create an unduly onerous burden on business operations.

To maintain the viability of direct marketing activities, which the Privacy Commissioner for Personal Data (PCPD) acknowledges is a useful service to consumers, the option should be made more straightforward – the data subject either elects to opt out from the use of the subject's data for direct marketing activities altogether, in which case he/she will not receive any direct marketing information, or, if he/she does not opt-out, full direct marketing information will be provided.

While we do not dispute with the requirements for the Personal Information Collection Statement (PICS) to be reasonably specific and readable, we question whether they should be made part of the legislation since reasonableness in this context has to be determined having regard to the facts and circumstances on a case-by-case basis. This

[1] "Person-to-Person Telemarketing Calls", UCAC Paper 1/2010, available at http://www.ofta.gov.hk/en/ad-comm/ucac/paper/uc2010p1.pdf

seems more appropriately to be addressed by codes of practice or guidelines issued by the PCPD.

Proposal (2): Unauthorised Sale of Personal Data by Data User

We do not see that strong arguments have been put forward to justify criminalisation of unauthorised sale of personal data. In fact, the report points out that the laws in the UK, Australia and New Zealand do not criminalise such sale. In the absence of good justification, it is not clear why Hong Kong would wish to be out-of-line with sound and strong jurisdictions.

We agree with the report that any new requirements for data users should be applicable to all users, irrespective of the amount of data held. As pointed out in the report, it would be difficult to impose higher standards on companies said to be in possession of so-called "pan-community personal data" as it is almost impossible to define what constitutes "pan-community personal data".

Proposal (3): Disclosure for Profits or Malicious Purposes of Personal Data Obtained without the Data User's Consent

We do not in principle object to the criminalisation of disclosure for malicious purposes but the penalty should be restricted to cases with a degree of culpability that warrants a criminal sanction, such as where there has been an intentional and blatant disregard of privacy rights with serious consequences. Thus, it is important to define the term "for malicious purposes" (if this is to be the test for imposing criminal sanction) appropriately to exclude inadvertent acts and to avoid unintended interference with normal legitimate commercial activities. In particular, the mere fact that the data user is remunerated ("with a view to gain for oneself or another") should not qualify as "malicious purposes" as proposed.

We would reiterate our argument in the last submission that any amendment to the PDPO and additional sanctions should be contemplated only if existing legislation is inadequate for dealing with the issue.

Proposal (5): Regulation of Data Processors and Sub-contracting Activities

We remain of the view that if greater regulation on data processors as subcontractors is needed, the government should consider imposing specific duties and obligations directly on data processors.

In any case, if the government decides to require data users to ensure that their data processors and sub-contractors comply with the PDPO, the duties and obligations to be imposed on data users must be reasonable and practicable. For example, the reference in the proposal to require a data user to use "other means", in addition to contractual means, to ensure compliance on the part of their sub-contractors is too vague. Data users cannot practically be expected to proactively and continuously oversee or monitor the performance of data processors to ensure compliance. Not only will this create an unduly

burdensome obligation on data users but this will also significantly reduce the business efficacy and cost-effectiveness of any sub-contracting arrangement.

We thus suggest that it should be a defence against an enforcement notice as long as the data user is able to demonstrate that appropriate contractual provisions are in place and that the data user has taken reasonable and practicable steps to enforce those provisions.

Proposal (7): Legal Assistance to Data Subjects under Section 66

The implementation of this proposal will likely result in more legal proceedings and we do not believe a sufficiently strong case has been built to justify the spending of public funds to subsidize these civil claims. However, if the proposal is to be implemented, there must be adequate safeguards against abuse of the system and clear conditions should be prescribed which must be satisfied before the PCPD may exercise this power. In addition to those factors included in the recommendations, we believe that a means and merits test should be imposed to avoid wasting public funds.

Proposal (14): PCPD to Disclose Information in the Performance of Functions

If the PCPD and his prescribed officers are to be permitted to disclose information necessary for the proper performance of their functions, this should be carefully and narrowly drafted to specify clearly the circumstances under which such disclosure may be made. In particular, disclosure should not be permitted where it might harm the legitimate business and other interests of the person to which the information relates.

<u>On Proposals Not to be Taken Forward</u>

We welcome the Government's decisions not to take forward a number of proposals discussed during the 2009 consultation exercise, in particular the following:

(i) to impose more stringent regulation on "Sensitive Personal Data" (Proposal no.38);

(ii) to empower the Office of the Privacy Commissioner for Personal Data ("PCPD") to "Award Compensation to Aggrieved Data Subjects" (Proposal 40); and

(iii) to empower PCPD to "Impose Monetary Penalty on Serious Contravention of Data Protection Principles" (Proposal 42).

Regulatory bodies, like many bureaucracies, tend to seek wider powers. But we have not seen a full justification provided for a drastic expansion of the PCPD office's powers, especially with respect to the powers to award compensation and impose penalty. There is no strong evidence that the present system is not working effectively to serve its purpose.

- END -