This document is downloaded from CityU Institutional Repository, Run Run Shaw Library, City University of Hong Kong.

Title	Personal data protection in Hong Kong: Problems and solutions
Author(s)	Chiu, Ka Min Peter (趙嘉銘)
Citation	Chiu, K. M. P. (2011). Personal data protection in Hong Kong: Problems and solutions (Outstanding Academic Papers by Students (OAPS)). Retrieved from City University of Hong Kong, CityU Institutional Repository.
Issue Date	2011
URL	http://hdl.handle.net/2031/6457
Rights	This work is protected by copyright. Reproduction or distribution of the work in any format is prohibited without written permission of the copyright owner. Access is unrestricted.

LW 4635 Independent Research

Personal Data Protection in Hong Kong: Problems and Solutions

Chiu Ka Min Peter
Year 4 LLB
SLW 330

Word Count: 9604

I. Introduction

Credit-card services, fitness club membership, boutique VIP membership, magazine subscription services, outward bound training camps; we always give out our personal data in making applications for these services; yet seldom do we ask for what purposes the data are collected, and how they are going to be processed. It is only until recently when the media reported that Octopus, a company that provides smart-card services in Hong Kong, collected the personal data of its customers and sold it to a number of other companies, which brought nuisance to the customers when they made direct-marketing calls to them. A few questions come up to our minds. Is Octopus allowed to sell the data or is there some sort of protection which restricts the transfer of our personal data? And if such sale is prohibited, what can we customers do about it?

In view of the recent Octopus case, this article will explain the problems of the current personal data protection regime in Hong Kong, with reference to the situation of transferring personal data to third parties. It will also suggest possible solutions. The structure of this article is as follows. In Part II, it will provide details of the Octopus case. Specific references will be drawn to the terms and conditions provided on the application form which collected the personal data to illustrate how companies respond to the current legislation. In Part III, it will introduce the relevant principles under the current Personal Data (Privacy) Ordinance[1] ("PDPO"). The scope, the standard of protection, and the enforcement mechanism with reference to any breach of the PDPO by illegal transfer of personal data to third parties will be explained. In Part IV, the problems of the current system will be explained by analysing the statues and the case law in the above three aspects. In particular, first, it will argue that the exclusion of anonymous data from the scope of the PDPO may frustrate the intention of the PDPO. Second, in terms of the standard of protection, the PDPO and its case law do not provide a definite answer to the extent of the duty borne by the data users; and the no-consent model under the PDPO does not provide adequate protection. Third, the enforcement mechanism through pursuing civil claims in courts is impractical and unjust because both the potential profit by breaching the statutory requirements and the cost of the litigation is grossly disproportionate to the fruit of success in such a claim. In Part V, it will suggest solutions to the identified problems. It will borrow the

[1] Cap 486.

rationale of existing legal machinery from other areas of law and explain how they can be fitted into the current regime.

II. The Octopus Card saga

The Octopus group of companies operates the Octopus smart card payment system in Hong Kong. The system started in fare payments on public transports and expanded to the retail sector in 2000.[2] It has a market share of 95% of the local population.[3] Octopus Holdings Limited operates its business through six fully-owned subsidiaries. Octopus Cards Limited operates the core business of the electronic payment systems. Octopus Rewards Limited runs the "Octopus Rewards Programme."[4] Under the programme, registered octopus card users can earn points by presenting their octopus cards while purchasing at certain shops. Users can later spend the points on redeeming other goods and services from Octopus' business partners.[5]

In July 2010, a person who claims to be a former employee of an insurance company reported to the media that the company has purchased personal data of over two million Octopus users for promotional use.[6] The insurance company was one of the business partners of Octopus which provides benefits for Octopus users participating in the Octopus Rewards Programme. After wide media coverage on the incident, the Privacy Commissioner for Personal Data commenced investigation pursuant to s38(b) of PDPO for any violations of the data protection principles.

The details of the programme were revealed during the investigation. Personal data of the users joining the programme were collected from the registration form. It is mandatory for the applicant to provide his name, Hong Kong Identity Card number, date of birth and other contact details, which were used mainly for customer authentication as claimed by Octopus. In addition,

---

[2] Octopus Holdings Limited, 'Our History' <www.octopus.com.hk/about-us/corporate-profile/our-history/en/index.html> accessed 11th February 2011.

[3] Octopus Holdings Limited, 'Services in Hong Kong' <www.octopus.com.hk/about-us/corporate-profile/services-in-hong-kong/en/index.html> accessed 11th February 2011.

[4] Office of the Privacy Commissioner for Personal Data, 'The Collection and Use of Personal Data of Members under the Octopus Rewards Programme run by Octopus Rewards Limited' Report Number: R10-9866 ("the Investigation Report").

[5] Octopus Holdings Limited, 'How does it work?' <www.octopus.com.hk/earn-and-redeem-rewards/how-does-it-work/en/index.html> accessed 11th February 2011.

[6] The Standard, 'Octopus in hot water over "sold" personal data claim' 15th July 2010.

the registration form also asks for other information, such as, marital status, educational level, occupation, monthly personal and household income, but these are optional. According to Octopus, the information requested in the optional fields is for the provision of "promotional benefits" to members.[7] Although there is no evidence suggesting that Octopus itself has used the data for direct marketing purposes,[8] Octopus did not deny that it has sold the personal data to six other companies for direct marketing purposes. It admitted so[9] and the transfer involved the personal data of more than two million registered users. In particular, Octopus received revenue of over 40 million dollars in its transaction with CIGNA.[10] In addition, the wordings on the terms and conditions of the registration form seem to suggest that Octopus has contemplated the transfer (or sale) of personal data to its partners. It was only a question of whether Octopus could gain the consent of the applicants using the terms and conditions on the registration form.

Two clauses on the registration form are of particular relevance. Clause 6.3 of the terms and conditions reads:[11]

> "You agree that all the personal information and data provided to us and all information related to the use of your Membership Octopus may be used by us for:…
>
> (b) providing you with carefully selected offers, promotions and benefits by us, our subsidiaries, our affiliates and/or Our Partners. We, our subsidiaries, our affiliates and Our Partners may need to carry out matching procedure (as defined in the Ordinance) to enable us/them to better understand your characteristics and to provide other services better tailored to our needs (such as offering special birthday promotions to you), to assist us and our Partners in selecting goods and services that are likely to be of interest to you and to establish whether you already have a relationship with our selected partners;
>
> …
>
> (j) as a source of information and data for other related purposes."

---

[7] The Investigation Report para. 3.5.
[8] The Investigation Report para. 3.41.
[9] The Investigation Report para 3.31.
[10] The Investigation Report para. 3.33.
[11] The Investigation Report para. 3.21.

By Clause 6.3(b), the applicant agrees to the transfer of his personal data to "Our Partners." The term is defined in Clause 2 as "business partners who wish to offer you benefits and targeted offers or redemption offers." It means that Octopus seeks to gain the applicant's consent to the transfer (or sale) of personal data to third parties, e.g. CIGNA. Furthermore, Clause 6.3(j) acts as a catch-all provision which seeks to give Octopus the authority to use the data for "other related purposes." It is unclear what "other related purposes" could have included, but in this context, its functions seem to be to allow Octopus to evade or avoid liability relying on this clause.

Further in Clause 6.4, it states:[12]

> "Data held by us relating to you will be kept confidential by us, but you agree that for the purposes set out in clause 6.3, we may transfer or disclose such information to the following parties (whether within or outside Hong Kong): …
>
> (b) any other person under a duty of confidentiality to us including our subsidiaries, our affiliates and Our Partners; and
>
> (c) any person to whom we, our subsidiaries, our affiliates or Our Partners is under a binding obligation to make disclosure under the requirements of any law, rule and regulation, including those of countries outside of Hong Kong for data transferred to those countries, but such disclosure will only be made under proper authority."

Octopus has adopted a similar approach in drafting the terms and conditions in this clause. The use of "any other person" and "any person" can cover a wide range of persons. If read together with Clause 6.3(j), since Octopus can be used for "any related purposes," clause 6.4 basically would impose no restriction to how Octopus can transfer the personal data collected.

Furthermore, given the severity of what the applicant can probably agree to on signing the application, the degree of notification of these terms does not seem proportionate. Very small fonts were used (1mm x 1mm for English and 2mm x 2mm for Chinese) and the whole clause was cramped into one single paragraph.[13] It is not only difficult for a normal applicant to comprehend the meaning of the clauses; it is perhaps even more difficult to read the text itself.

---

[12] The Investigation Report para 3.23.
[13] The Investigation Report para 3.25.

III. The current regulatory regime under the PDPO

The PDPO is currently the only enactment in Hong Kong which governs the processing of personal data. The PDPO was enacted in 1995 and was brought into force in 1996. The right to privacy provides the foundation of data protection.[14] The right is enshrined the Bill of Rights Ordinance.[15] It provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy…" and "everyone has the right to the protection of the law against such interference or attacks." The regulatory regime can be explained in three parts, i.e. the scope of application, the standard of protection and how the standards are enforced.

Scope

While there are enactments which provide for data protection in specific situations, e.g. secrecy provision under the Banking Ordinance,[16] the PDPO's scope is wide and is applied generally across most situations. The scope of the PDPO is set by the meanings of "data users", "data subjects" and their "personal data." "Data users" and "data subjects" are defined relation to "personal data."[17] "Data subjects" refer to individuals who are the subjects of the data. "Data user" is defined as a person who, either alone or jointly or in common with other persons control the collection, holding, processing or use of the data. While "data subjects" can only be real persons as personal data is limited to that of a "living individual," "data user" can be a body corporate as "person" includes any body of persons, corporate or unincorporated.[18] Furthermore, with regards to s65 PDPO, the actual scope of the definition of "data user" is wider than as defined in s2. Section 65 imposes vicarious liability on employers and principals of agents except in criminal proceedings.[19] An act done in the course of the employment or by a person as agent for the person with the authority shall be treated as an act done by the employer or the principal. Therefore, the definition of "data user" would not assist anyone attempting to avoid liability using the corporate veil. In the context of the Octopus case, the applicants are the "data

[14] Stefan Lo, *the Annotated Ordinances of Hong Kong Personal Data (Privacy) Ordinance (Cap 486)* (LexisNexis 2006) p. 1.
[15] Art 14 s8 Hong Kong Bill of Rights Ordinance (Cap 383).
[16] Section 120 Banking Ordinance (Cap 155).
[17] Section 2 PDPO.
[18] Section 2 Interpretation and General Clauses Ordinance (Cap 1).
[19] Section 65(4) PDPO.

subjects" and Octopus Rewards Ltd is the "data user." Octopus Holdings Ltd will be vicariously liable for its subsidiaries' acts.

The PDPO only covers personal data in recorded form. The definition of "personal data" relies on that of "data," which is defined as any representation of information in any document.[20] The data has to be in writing or in other recorded form such as data stored in a disc, or a tape. In addition, it was held in *Eastweek Publisher Ltd* v *Privacy Commissioner for Personal Data*[21] that photographs constitute pictorial representation of information, and may therefore also constitute representation of information. For "data" to qualify as "personal data", it must satisfy a three-limb test. The data must

a. relate directly or indirectly to a living individual;
b. from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
c. in a form in which access to or processing of the data is practicable.[22]

In the first limb, the document will be treated as directly or indirectly related to an individual if it falls in a continuum of relevance or proximity. The court will consider whether the information was significantly biographical and whether the data subject was the focus of attention.[23] In the case of situations similar to that in the Octopus card incident, the data will undoubtedly fall within the first limb. The scope of the second limb however is not as straightforward. Where the information in issue does not include the name of the data subject, the position is more obscure. In *Shi Tao* v *Privacy Commissioner for Personal Data*,[24] the defendant Yahoo! disclosed user registration information, IP address and certain e-mail contents of the claimant to Chinese authorities. The disclosure later led to the arrest and imprisonment of the claimant. It was held that the information disclosed did not *ex facie* reveal the identity of the claimant. It was not reasonably practicable to ascertain the identity of the person using the computer with only the information disclosed. This case has left in doubt the issue of whether, or under what circumstances anonymous data can fall within the scope of the PDPO. The "registration

[20] Section 2 PDPO.
[21] [2000] 1 HKC 692.
[22] Section 2 PDPO.
[23] *Durant* v *Financial Services Authority* [2003] EWCA Civ 1746.
[24] [2008] 1 HKC 287.

information" disclosed could actually include the gender, date of birth or even the name of the claimant had he not elected to send the email under an alias.[25] The case has to be contrasted with *Cinepoly Records Co Ltd & Ors* v *Hong Kong Broadband Network Ltd & Ors*,[26] which was distinguished in *Shi Tao* for involving a "different factual matrix." In *Cinepoly*, it was held that where the IP address, coupled with the more reliable personal information which is in the possession of the internet service providers, can constitute personal data under the PDPO. Therefore the court in *Shi Tao* probably did not treat IP address and other relevant information as personal data because there was no guarantee that the information provided was genuine,[27] and furthermore in this unfortunate case, the claimant could not testify that he has given true information; nevertheless, whether personal information short of the name of the data subject falls within the scope of the PDPO is not without doubt. The third limb of the test refers to the retrievability of the data. The third limb recognised that irretrievable data may pose only negligible risk to the individual.[28]

Standard of protection

The use of personal data is primarily regulated by the six data protection principles. Data users are not allowed to engage in act or practice which contravenes a data protection principle.[29] Transfer of personal data by virtue of the definition of data users which include persons who transfer the personal data are regulated by the data principles. The data protection principles are set out in Schedule 1. They concern:

Principle 1 – purpose and manner of collection of personal data

Principle 2 – accuracy and duration of retention of personal data

Principle 3 – use of personal data

Principle 4 – security of personal data

Principle 5 – information to be generally available

Principle 6 – access to personal data.

---

[25] [2008] 1 HKC 287 at 300.
[26] [2006] 1 HKC 433.
[27] [2008] 1 HKC 287 at para 65.
[28] Mark Berthold and Raymond Wacks, *Hong Kong Data Privacy Law* (2nd edn Sweet & Maxwell 2003) p. 213.
[29] Section 4 PDPO.

Since the issues involved in the Octopus case concerns the collection of personal data through application forms provided by the data user and the subsequent sale of them. Principle 1 and Principle 3 are particularly relevant because they regulate the manner of collection and the use of personal data after collection respectively. Principle 1(3)(b) requires that the data subject has to be explicitly informed, on or before collecting the data, of the purpose (in general or specific terms) of collection and the classes of person to whom the data may be transferred. The imperative under this principle is to duly inform, whether the data subject has in fact been informed; in other words, whether he has given consent, is not an issue. In the Octopus case, it applies at the time when the data was collected. This notification requirement can be fulfilled by taking reasonably practicable steps. The notification requirement has to be complied even where non-compliance can result in greater convenience and lower costs on the part of the data subjects.[30]

As for Principle 3, the imperative is not to use the data for other purposes. The data user has to act in accordance with this principle at all time after the collection of the data. The data can be used for other purposes only if it is a "directly related purpose" or the data user has obtained "prescribed consent" from the data subjects. Paragraph (a) and (b) operate only when the data user is seeking to use the data for purposes which were not to be used at the time of collection. In the Octopus case, once the application form has been submitted, if Octopus is using the personal data for non-related purposes, it would be required to seek consent from the data subjects. A data subject who does not reply to Octopus' intended change of purpose of using his personal data will not be taken as giving consent.

Enforcement

Where a data user has committed a breach of the data protection principles, the PDPO provides mainly two methods of enforcement. First, the Commissioner can issue enforcement notice to compel compliance with the data protection principles. Second, aggrieved parties can commence a civil action to seek remedies for any damages caused through the courts.

---

[30] Stefan Lo, *The Annotated Ordinances of Hong Kong Personal Data (Privacy) Ordinance (Cap 486)* (LexisNexis 2006) p. 137.

The Commissioner is given the power to conduct investigation for any breaches of the data protection principles under the PDPO.[31] Usually where a breach is found upon the end of the investigation, the Commissioner may issue enforcement notice if the data user is contravening or may continue to contravene any data protection principles. While the Commissioner is not bound to issue an enforcement notice where there is a breach, it must consider whether the contravention has caused any person damage or distress.[32] This provides an indirect mechanism of enforcement. Breach of a data protection principle *per se* does not constitute a criminal wrong,[33] but where an enforcement notice has been served to compel compliance, contravening the enforcement notice is an offence punishable with imprisonment.[34] Under the UK model, of which the mechanism of enforcement is similar to that in Hong Kong, enforcement notice procedure is usually taken as the last resort. Other methods of promotion of observance of data protection principles such as consultative or advisory process are preferred.[35]

The Commissioner's power to resolve the dispute however does not extend to ordering any remedies for the aggrieved parties besides enforcement notice. In *Chan* v *Privacy Commissioner for Personal Data*,[36] it was held that the Commissioner is not empowered under the PDPO to demand an apology or compensation. Section 66 of the PDPO allows data subjects who have suffered damage by reason of a contravention, including a breach of any data protection principles, to seek compensation through the courts. In general, damages cover both pecuniary and non-pecuniary losses such as pain or suffering.[37] Injury to feelings is expressly included as a kind of damage which compensation can be sought under section 66.[38] In *Campbell* v *Mirror Group Newspapers*,[39] the claimant sought compensation following publications which relate to her drug addiction. In addition to £2,500 of damages for distress (which is not recognised under the PDPO) and injury to feelings, £1,000 of aggravated damages was awarded. Besides

[31] Section 38 PDPO.
[32] Section 50(2) PDPO.
[33] Section 64(10) PDPO.
[34] Section 64(7) PDPO.
[35] Abu Baker Munir & Siti Hajar Mhod. Yasin, *Privacy and Data Protection* (Sweet & Maxwell 2002) pp. 163 – 164.
[36] Administrative Appeal Board, No. 4/1997.
[37] Rosemary Jay & Angus Hamilton, *Data Protection Law and Practice* (2nd edn Sweet & Maxwell 2003) p. 352.
[38] Section 66(2) PDPO.
[39] [2004] 2 AC 457.

monetary compensation, depending on the venue of the action, the Court of First Instance may also invoke its inherent power to grant equitable remedies in addition to the compensation sought under the PDPO.[40]

IV. Problems of the current system with regards to the transfer of personal data

The Octopus case indicated that the current regulatory system is insufficient to protect data subjects from the harms that may arise from the transfer of their personal data. The fact that the Commissioner has conducted a hearing and ruled against Octopus should not be seen as an effective implementation of the system. The current regulatory system in Hong Kong suffers from three major problems in its scope, standard of protection and enforcement mechanism respectively.

Scope – exclusion of anonymous personal data

PDPO's protection does not cover cases where anonymous data has been submitted or transferred. Anonymous data are data which but for a lack of the data subject's name would have been treated as personal data under the PDPO. As illustrated in the above cases, anonymous data falls outside of the protection of the PDPO or the position of it is at least unclear. The EU Directive also supports the interpretation that anonymous data is not protected.[41] While no issues concerning anonymous data has surfaced in the Octopus case, as Octopus has admitted that the names of the participants of the schemes have both been collected and transferred, this unclear or insufficient definition of personal data may frustrate the objective of the PDPO.

The exposure of anonymous personal data can cause the same type of harm which the PDPO is intended to protect data subjects from. The objective of the PDPO was to "protect the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith."[42] The harm created by violation of privacy can be understood in two dimensions. First, intrusion to privacy *per se* is recognised as a kind of harm on the autonomy of individuals. This is reflected in the Australian Privacy Charter, "A free and democratic society requires respects for the autonomy of individuals…" It is of the nature of a breach of a fundamental right.

[40] Rosemary Jay & Angus Hamilton, *Data Protection Law and Practice* (2nd edn Sweet & Maxwell 2003) p. 355.
[41] Rosemary Jay & Angus Hamilton, *Data Protection Law and Practice* (2nd edn Sweet & Maxwell 2003) p. 79.
[42] Long title PDPO.

Second, privacy is "the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others."[43] Besides the fact that it is a breach of a right, exposure of one's private life beyond the extent to which he has consented can cause actual harm to the person. For example, exposure of one's sexual orientation can cause emotional distress. These two types of harm are not dependent upon whether the data exposed is named or anonymous. The first type of harm is a breach of a fundamental right. The second type of harm is caused when the fact of exposure comes to the knowledge of the data subject. It does not depend upon whether the data itself is named, but whether the person himself has perceived the exposure.

As in the Octopus case, the sale of customers' personal data to third parties for unsolicited promotional services caused nuisance to the customer. While direct marketing call is a matter of nuisance and does not strictly relate to protection of personal data, the second type of harm is brought into the picture if the company holds and makes use of the personal data of the customer in these calls. Octopus collects all the essential personal data of the data subjects, including their names using the application forms. The sale of the personal data will normally be regulated by the PDPO. But if Octopus deleted the names from the personal data and sell it to third parties, under the current position, it would seem that the transfer will fall outside the scope of the PDPO. Both the transfer and the subsequent use, e.g. for direct marketing purposes, of the data will not be regulated by the PDPO. The first type of harm is caused upon exposure. The second type of harm is brought to a data subject when a stranger on the phone, who is in possession of all the personal details of the data subject, mentions the personal data which the data subject has provided on the application form. This is particularly disturbing if the data mentioned are of an intimate nature.

Therefore, the requirement of the legislation will be easily circumvented to facilitate sale of personal data, which would otherwise be unlawful, if anonymous data is excluded from the scope of the PDPO.

Standard of protection – a confusing standard and one which ignores the consent of individuals

[43] Abu Bakar Munir & Siti Hajar Mohd. Yasin, *Privacy and Data Protection* (Sweet & Maxwell 2002) p. 2.

There is insufficient protection guaranteed by the current data principles with regards to issues relating to transfer of personal data. Two points in relation to the data protection principles are unclear. In addition, the data protection principle has ignored the question of the data subject's consent.

Principle 1(3) imposes a notification requirement on the data user. It has to take all practicable steps to ensure that the data subject is explicitly informed, on or before collecting the data, of the purpose (*in general or specific terms*) for which the data are to be used; and the classes of persons to whom the data may be transferred.[44] The standard of "general or specific" is confusing. Stating the purpose in specific terms is obviously a requirement higher than stating it in general terms. Statutory requirements should not have two standards at the same time unless they are intended to be applied in different situations; e.g. a lower requirement may be applicable to data users which are less financially resourceful, yet no such specifications are made or can be inferred from the principle. As a result, the requirement of stating the purpose "in specific terms" becomes redundant as it can be fulfilled by satisfying the alternative lower threshold. Therefore, contrary to the opinion of the Commissioner, it is arguable that the catch-all provision concerning the purpose of use of the data in the terms and conditions in the Octopus case has not violated the notification requirement under Principle 1. The Principle will not be able to protect data subjects' right to know for what purpose their personal data will be used.

Divergent approach can also be seen in the interpretation of the scope of "directly related purpose" under Principle 3(b). In *Tse Lai Yin Lily* v *Incorporated Owners of Albert House*,[45] there was a fatal accident involving the collapse of a canopy. In allowing a discovery order on the witness statements taken by the police after the accident, it was held that bringing a civil action for damages in relation to the collapse was a purpose directly related to the original purpose, i.e. police investigation. The case has not provided a clear test on what "directly related" means but it was stated that "the nexus of that relationship is the collapse of the canopy."[46] A different test of "reasonable expectation" however is adopted in the investigation by the Commissioner. The Commissioner relied on the Administrative Appeals Board's decision

[44] Data Principle 1(3)(b) Schedule 1 of PDPO.
[45] [1999] 1 HKC 386.
[46] [1999] 1 HKC 386 at 393.

in *Wing Lung Bank Ltd* v *Privacy Commissioner for Personal Data*.[47] The Commissioner opines that the average customer; who forms the majority, will regard the scheme as merely a customer loyal exercise. Therefore it was decided that sale of data for profit was not a directly related purpose. The foci of the two tests are different. The "nexus" test looks at the objective relationship between the two purposes. While the "reasonable expectation" test; although it is an objective test, the starting point is the point of view of the data user. While the Commissioner favours the latter test, its opinion does not represent or help to clarify the judicial position in this regard. Problems may arise in applying the "nexus" test in the Octopus case given its low threshold.

Unlike the Data Protection Act 1998 in the United Kingdom, which allows data subjects to consent to non-compliance with the statutory requirements,[48] consent of the data subjects to the collection and subsequent use of the personal data rarely play any role under the PDPO. The need to obtain "prescribed consent" under Principle 3(b) arises only when the data user seeks to alter the use of the data after collection. The intention of the legislation to exclude consent of data subjects from the data protection principles was to offer better protection. The requirements are made mandatory so that data subjects will not be able to opt-out the protection by the PDPO when bargaining power is unequal.[49] Despite its good intention to provide a fairer data protection mechanism, the "no consent model" under the PDPO has however ignored the need to obtain real consent from data subjects with respect to data collection and uses. Behind the principles requiring data subjects to provide notification to data user as to the purpose of collection, the PDPO seeks to allow data subjects to make an informed decision as to whether they will submit their personal data.[50] By taking out the element of consent, the focus of the PDPO was placed on the extent to which data user has to inform the data subjects (as required under Principle 1), but not the extent to which data users are in fact informed. Notification requirement under Principle 1(3) nevertheless implies the necessity of consent from the data subjects as it is applicable only in situations where the data user supplies the data as distinct from

[47] [2010] 6 HKC 266 at para 20.
[48] Sch 1 para. 1(a); Sch 2 para. 1 Data Protection Act 1998.
[49] Mark Berthold & Raymond Wacks, *Hong Kong Data Privacy Law* (2nd edn Sweet & Maxwell 2003) p. 202.
[50] Mark Berthold & Raymond Wacks, *Hong Kong Data Privacy Law* (2nd edn Sweet & Maxwell 2003) p. 240.

data subjects collecting the data by its own observations.[51] In view of the fact that data subjects are not usually notified even after data users have taken steps to notify, such as in the Octopus case, inserting them in small prints on the terms and conditions which applicants seldom read, the no consent model fails its objective to ensure that the data user has made an informed decision.

Enforcement – a civil claim mechanism which provides insufficient remedies

The PDPO enforcement mechanism lacks practicality and causes injustice in the Octopus type of cases. The claim initiated by two of the members of the scheme shows how the PDPO causes these problems by failing to providing sufficient remedies for the aggrieved parties.

Soon after Octopus' sale of personal data was exposed by the press, two members of a political party in Hong Kong filed claims at the Small Claims Tribunal in October 2010 under section 66 of the PDPO as compensation for the sale of their personal data.[52] The amount they claim was exceptionally low; namely $50 each, injury to feeling included.[53] The low amount of damages might be a result of traditional common law's attitude towards damage to privacy. Privacy has not been valued as much as in other European cultures and this type of loss is more likely to give rise to opening a floodgate of claims than other injuries which are more "real." This type of loss has the lowest position in the hierarchy of types of loss, for which remedies are rarely provided unless they are consequent on a damage of a more recognised type, such as personal injury and property damage.[54] In any event, the provision for compensation of injury to feeling cannot assist the claimant much in this case as the personal data involved only concerns some basic information of the data subject but does not concern any intimate part of his life. Although there have been cases where a higher amount of damages was awarded for distress[55] and injury to feelings, as in *Campbell* v *Mirror Group Newspapers*,[56] £2,500 were awarded, but the facts are

[51] *Eastweek Publishing Ltd* v *Privacy Commissioner for Personal Data* [1999] HCAL 98/1998. See also Mark Berthold & Raymond Wacks, *Hong Kong Data Privacy Law* (2nd edn Sweet & Maxwell 2003) p. 239.
[52] *Wong Wing Kit* v *Octopus Holdings Limited & Octopus Rewards Limited* SCTC 36611/2010.
[53] The Standard, 'Cardholders file $50 Octopus claims' <http://www.thestandard.com.hk/news_detail.asp?pp_cat-30&art_id=101430&sid=29163832&con_type=1> accessed 11th February 2011.
[54] David K. Allen, *Damages in Tort* (Sweet & Maxwell 2000) p. 6.
[55] Damages for distress was available under the Data Protection Act 1998 in UK. The PDPO does not provide so.
[56] [2002] EWHC 499 (QB).

too different from the Octopus case. The claimant in *Campbell* was a public figure and the personal data involved concerns her attendance at a drug addiction treatment centre. Due to the nature of the personal data concerned and the fact that the data in the Octopus case is not publicised but transferred to specific third parties along with the personal data of millions of others, the Octopus claim would be far from comparable to the case of *Campbell*. Despite the low amount of claim, Octopus intends to defend it, stating that it might seek judicial review against the Commissioner's decision.[57] The claimants have also been warned by the adjudicator that subsequent appeals of the case could end in the Court of Final Appeal, involving massive legal fees.[58] The costs involved in the proceedings are grossly disproportionate to the fruit of success, to the extent that but for the claimant's political intentions, it is unlikely that any ordinary claimant would initiate or continue to pursue the claim. Given the fact that the Commissioner has no authority to order any remedies for the data subjects, the enforcement mechanism of the PDPO is impractical in these types of cases.[59] Bringing a civil claim under s66 is impractical as it does not provide a cost-effective method of enforcement against a wrongful data user. The exceptionally low amount which can be claimed cannot provide the incentive for potential claimants to initiate an action to recover for their losses.

The problem of disproportion between the costs and the potential claim would not have been a problem of the enforcement mechanism under the PDPO but a question of how the civil justice system can be made more cost-effective had it not been the fact injustice is caused as a result of the inadequacy of damages. The Octopus case involves mass collection of personal data and subsequent sale of it. The personal data are not of particularly important value to the individual; in other words, they are not of high intimacy as in the *Campbell* case. The value of the personal data of an individual is low. But when the data subject collects the data in mass, the product of the mass collection carries business value for marketing or statistics purposes. In the Octopus case, more than 40 million dollars of revenue was generated. The amount would probably be higher than the damages Octopus had to pay even if it settled all the claims from members of the

[57] Sun Daily, '獎賞公司洩私隱八達通擬覆核' (Octopus Reward Ltd leaked personal data, Octopus contemplating judicial review) <http://the-sun.on.cc/cnt/news/20101229/00412_003.html> accessed 11th February 2011.
[58] RTHK, 'Legal fees warning in Octopus case' <www.rthk.org.hk/rthk/news/englishnews/20100904/news_20100904_56_696075.htm> accessed 11th February 2011.
[59] See above.

Scheme. Therefore, the problem caused by the low amount of damages payable is not only one which dissuades potential claimants from enforcing their rights; but in addition, it is a problem of injustice as the PDPO allows data subjects to profit from the a recognised wrong under the regime itself.

V. Solutions

The following paragraphs will introduce the proposed solutions to the problems identified above and the reasoning behind these solutions.

Scope – semi-transparent approach to define personal data

The exclusion of anonymous data from the definition of "personal data" creates a loop-hole in the PDPO as it is likely that the statutory requirements can be circumvented by simply excluding the name of the individual. Modification of the current definition is needed in two aspects.

Clarification should be made under the second limb of the test of "personal data." Namely, when determining whether it is practicable for the identity of an individual can be ascertained from the data, the mere fact that the name of an individual or any personal identifier cannot be ascertained from the data should not render the data impossible to be recognised as "personal data" under the PDPO. "Personal identifier" is also included because it bears similar character as the name of an individual in a personal data system.[60] It is also an unique identifier and is included in order to prevent confusion. The aim of this clarification is to address the problem that the same kind of harm can result from a leakage of data. Harm has long been recognised as a criterion determining whether legislation is needed. In the context of a liberal society like Hong Kong, as John Stuart Mill has stated, "the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others."[61] If the PDPO's objective is to prevent the harm caused by breach of privacy, it should not distinguish whether the data is named or anonymous if the resulting breach of privacy is of the same kind. Whether the name of the individual is included does not change the fact that there is a breach of

[60] Section 2 PDPO.

[61] Ian McLeod, *Legal Theory* (3rd edn Palgrave MacMillan 2005) p. 185.

an individual's privacy and the consequence of leakage of the data can be equally harmful to the individual.

Excluding the consideration of whether the name or any personal identifier is present leads to the second aspect of modification. After removing the need of the name of the individual, there remains a question of what then should the criteria of determining whether it is practicable to identity an individual be. The criteria can be deduced from dissecting the concept of harm as stated above. There underlies a notion behind the argument that the same kind of harm is effected whether or not the name is included. It is that the concept of a "person", in our world which is flooded and controlled by information, cannot be isolated from the "personal data" of that person. In other words, a person cannot be defined without referring to its personal data. It is impossible to identify a person without mentioning any of his characteristics or information, such as name, address, identity card number, appearance and so forth. The name of an individual is only part of his personal data. It is rarely unique. The data "John Chan" can refer to a lot of persons. By corollary, the concept of a person is only a conglomeration of all of its personal data. "A person" can now be understood as the perfect set of his personal data. Therefore the harm is the same because in both cases whether or not the data is anonymous, the harm is done to the set of personal data which can both sufficiently identify the person.

If the concept of "a person" is understood as the perfect set of his personal data, the question of whether it is practicable to identify an individual from the personal data in the possession of the data subjects thus become a matter of comparison between the two sets of data. A step-wise approach as in the three-limb test employed in the current PDPO is not preferred in interpreting what constitutes a "practicable identification" because there might be a multitude of factors of different weight depending on the specific facts of each case. The Control of Exemption Clauses Ordinance[62] ("CECO") provides an example of how the legislation can deal with this type of situations where there are a number of factors determining the result. The CECO restricts the incorporation of contractual terms seeking to exempt the seller's liability with respect to its obligations under the Sale of Goods Ordinance.[63] Such exemption clauses have no effect

[62] Cap 71.
[63] Cap 26.

between two persons dealing in the course of business unless the term satisfies the requirement of reasonableness.[64] In determining whether the requirement is satisfied, the CECO adopts a semi-transparent approach which directs the court to consider a number of factors where it appears to be relevant.[65] The semi-transparent approach of assessment in the CECO can be borrowed to provide the backbone of how the two sets of data are to be compared.

In considering whether an individual is identified, it is suggested that the factors below should be considered.

First, the amount of data related to the individual. This is a basic criterion because the more data related to the person is present, the more likely it is to match it with the perfect set of data of an individual. However, a high amount of general information which is also data of a lot of other individuals, e.g. gender, nationality, etc., is unable to assist the person in possession of the data to identify the data subject. Also, from the protection of privacy point of view, the more personal data is involved, the more serious the breach of privacy usually is. Second, how uniquely the data relates to the individual. Quantity does not imply quality. A higher amount of personal data does not always imply a higher likelihood of identification. On the other hand, information such as identity card number and personal mobile phone number are examples of personal data which does not require a high amount of them to identify an individual. Uniqueness of the data is therefore the second factor.

Third, if one departs from the match-making philosophy; namely, how one compares between two sets of personal data, and shifts the attention to protection of privacy, another factor will surface. Each piece of data in the set of data possessed by the data subjects can carry different values in terms how private it is. Some personal data by nature are more personal than the other. Taking the *Campbell*[66] case as an example, the "data" that the data subject is undergoing narcotics treatment is more private than some other aspects of her life. Given that the notion of privacy embraces the idea of to what extent individuals are willing to expose themselves to others, intimacy of the data should therefore be a relevant factor.

---

[64] Section 11(3) CECO.
[65] Schedule 2 CECO.
[66] *Campbell* v *Mirror Group Newspapers* [2004] 2 AC 457.

The focus of the discussion above is to address the problem of a lack of protection for anonymous data and the resulting harm. It is likely that there exist other factors which have not been mentioned yet should also be taken into account in assessing whether the data identifies an individual. Any of such factors should always reflect the principle to protect the right to privacy.

Standard of protection – clarifying unclear standards and bringing back consent

The ambiguity of the standard of protection can be cleared up by amending and supplementing the data protection principles with more specific provisions. Consent of a data subject to any transfer of his data should be brought back as a necessary element before any transfer can be made.

The impractical wordings of "general or specific terms" employed in Principle 1(3)(b) should be simplified. If any changes are to be made with respect these wordings, the requirement has to be either "in general terms" or "in specific terms to make any logical sense. It is suggested that data user should be required to explicitly inform the data subject of the purpose in specific terms only. This can effectively prevent any catch-all provisions like the one in the Octopus case, which explicitly inform data subjects nothing. A change in this requirement is unlikely to cause any hardship to data users who are less financially resourceful. Under the existing mechanism, data users are only required to take "all practicable steps" to inform. Practicable is defined as "reasonably practicable" in PDPO.[67] The court explained the term 'reasonably practicable" in *Tam Yuen Hoi* v *Chau Mu Cheng & Ors*[68] in the context of contractor's duty to ensure safety in construction site.[69] It was held that "what is reasonably practicable involves the balancing of risk on the one hand against the costs and inconvenience in providing the measures necessary for averting the risk on the other."[70] By analogy, "reasonably practicable" in the context of data protection would mean a balance of risk of between the consequences of inaction; namely, the risk of harm associated with data subjects not notified of the purpose, and the costs and inconvenience in giving such notification. Given that the costs and inconvenience of notification

[67] Section 2 PDPO.
[68] [2003] HKCU 927.
[69] Regulation 38A(1) Constructions Sites (Safety) Regulations (Cap 38A).
[70] [2003] HKCU 927 at para. 26.

will be taken into account, requiring notification to be made in specific terms in every case is unlikely to cause hardship.

As for the test what constitutes a directly related purpose under Principle 3(b), supplementary provisions should be inserted under Principle 3 to clarify the correct test. The danger of the "nexus" test is obvious. It implies that a data user does not have the obligation to notify a data subject of a purpose which may be completely concealed from the data subject; nevertheless related because it is part of a larger plan which a data subject has no knowledge of. Applying this "nexus" test to the Octopus card scenario, it is arguable that the "nexus" of the relationship between the original purpose of rewarding loyal customers and the "directly related purpose" of sale of personal data is the business scheme which involves the triangular relationship between Octopus, customers and the business partners. Customers provide personal data to Octopus. Octopus sells the data for profit to its business partners, and the business partners provide the rewards which the customers seek in the first place. As a result, under the "nexus" test, data users will be treated to have been notified of the transfer even where the linkage between the transfer and the original purpose is established by a scheme of which a data user can have no knowledge. It takes an omniscient point of view on the matter to what is directly related. It is suggested the "reasonable expectation" test is more realistic. In determining whether a purpose is directly related, the reasonable expectation of the data user should be considered. "Reasonable expectation" test allows the court take into account the specific situation in which the data is collected. The absurdity in implying knowledge of a hidden scheme to a data user will be prevented.

The no-consent model under the current regime is unable to guarantee an informed decision by a data subject with respect to transfer of its data. The rationale behind calling for more protection for data user in this regard is the inability on the part of the data subjects to appreciate the risk associated with providing their personal data. This inability to appreciate the risk is similar to some cases where a party to a contract pleads undue influence. *Royal Bank of Scotland plc* v *Etridge (No 2)*[71] provides an example of how a balance can be struck between the protection of the party failing to appreciate the risk and the interest of the party seeking to enforce the

[71] [2002] 2 AC 773.

agreement. The wife in the case argued that the surety agreement she executed in favour of her husband was made under his undue influence and was therefore voidable, so that the bank as a third party could not enforce the surety agreement against her. It was held that an evidential presumption of undue influence operates against the bank,[72] to the effect that the bank was "put on inquiry" whenever the relationship between the surety and the debtor is non-commercial.[73] Lord Nicholls articulated the specific steps to be taken by the bank,[74] satisfying of which the bank can rebut the presumption. The measures given in *Etridge* was to provide protection for the surety, who may be blinded by the trust and confidence he has in the debtor, against a serious risk which might be able to be deduced from the surety agreement but not actually not foreseen by the surety.

Although there is no relationship of trust and confidence between the data user and the data subject, a similar type of protection is needed in relation to transfer of personal data because in both situations first there is an underlying assumption that the data subject or the surety does not read the document, or if he reads, does not have the ability to understand the effect of the transfer or the surety agreement; and second the risks involved in giving consent are serious. It is suggested a similar mechanism should be employed in relation to transfer of personal data. The notification requirement in relation to any transfer of personal data shall be deemed to have not been met unless the prescribed consent with specific reference to the transfer has been obtained from the data subject. Inserting this requirement can switch the fundamental question in these cases back to one which inquires into whether the data subject has actually consented to the transfer. It is more sensible to ask to what extent the data subject has been notified rather than to what extent the data user has notified the subject. "Prescribed consent" is the standard to determine whether the data subject has been duly notified. The term is defined under the PDPO to mean express consent of the person given voluntarily except where such consent has been withdrawn subsequently in writing.[75] While the definition does not seem to add anything to the common law definition of consent or acceptance except that implied consent is excluded, it can provide the basis on which the Commissioner can issue code of practice on how prescribed

[72] [2002] 2 AC 773 at 797.
[73] [2002] 2 AC 773 at 814.
[74] [2002] 2 AC 773 at 804.
[75] Section 2(3).

consent is obtained while preserving the generality required in the data principles which have to accommodate a wide range of circumstances. Contravention of the code of practice will constitute proof of contravention of the data principles in the absence of contrary evidence.[76] It is not the aim of this article to spell out specifically what steps should be required under the code of practice. But in principle, the code of practice should provide a wide range of means to obtain prescribed consent, depending upon the nature of the transfer and the financial means of the data user. For example, in the Octopus type of cases, data users may be required to obtain the consent in writing in a separate document; on the other end of the spectrum, a simple oral confirmation may suffice.

The consent model suggested above will not remove the protection offered by the no-consent model. Data subjects under this model still cannot consent to opt-out the statutory requirements under the PDPO. Consent only becomes a necessary but not a sufficient element in proof of compliance of the notification requirement. The model nevertheless will not be a complete shield for data subjects against transfer of their data. Data subjects will still be forced to consent to the transfer if it is required by a monopolist in the market of an essential product or service. Whether this should be allowed warrants a separate discussion that may concern the necessity of competition law in Hong Kong and unfair trade, which is out of the scope of this article.

Enforcement – statutory authorisation of aggravated and exemplary damages

The low amount of compensation payable to the data subjects makes pursuing a claim under s66 infeasible and causes injustice. Breach of the data protection principles is an act similar to trespassory torts against another person as they both involve an intentional act which is considered wrongful in law. It is therefore suggested that aggravated and exemplary damages, which are available to the court in awarding remedies for intentional torts, should be made an available option to the court to consider when it finds a breach of the data protection principles in civil claims under s66 of the PDPO.

In general, these two types of damages are available in common law as remedies for trespassory torts and defamation. The rationale behind exemplary damages was explained in *Rookes* v

[76] Section 13 PDPO.

Barnard.[77] Lord Devlin provided three categories of cases where exemplary damages can be awarded:

1. Where there had been oppressive, arbitrary or unconstitutional action by the servants of the government;
2. where the defendant's conduct has been calculated by him to make a profit for himself; and
3. where exemplary damages are expressly authorised by statute.

For the second category, Lord Devlin explained that "where a defendant with a cynical disregard for a plaintiff's right has calculated that the money to be made out of his wrongdoing will probably layered exceed the damages, it is necessary for the law to show that it cannot be broken with impunity." The principle is further elaborated in *Broome* v *Cassell*.[78] The defendants in the case published a book which contains defamatory passage to which the claimant has objected at the early stage of publication. In spite of that, the defendants proceeded with only a few minor amendments. Exemplary damages were awarded. The court further explained that exemplary damages was not only to reflect the extent to which the defendant was unjustly enriched, but it has to be shown that the defendant is subjectively aware of the nature of his conduct and the likelihood of profiting from the wrong.[79] Therefore, exemplary damages is a remedy which is punitive in nature and focuses on the conduct of the defendant.

The principle of aggravated damages is however less clear. It is generally accepted that aggravated damages focuses on how much the plaintiff ought to receive rather than how much the defendant ought to pay.[80] It seeks to compensate for any injury caused to "the plaintiff's proper feelings of dignity and pride."[81] It is generally compensatory in nature. However it overlaps with exemplary damages as it also takes into consideration the conduct of the defendant. Dyson J. summarised the principle of aggravated damages as containing two elements.[82] First, there needs to be exceptional or contumelious conduct or motive on the part of the defendant in committing the wrong. Second, the defendant has suffered intangible loss of injury to

[77] [1964] AC 1129.
[78] [1972] AC 1027.
[79] David K. Allen, *Damages in Tort* (Sweet & Maxwell 2000) p. 123.
[80] *Broome* v *Cassell* [1972] AC 1027 per Lord Reid.
[81] *Rookes* v *Barnard* [1964] AC 1129.
[82] *Appleton* v *Garrett* [1996] PIQR P1.

personality. It was further stated in *Thompson* v *Commissioner of Police of the Metropolis*[83] that "there can be a penal element in the award of aggravated damages."[84]

The Sex Discrimination Ordinance[85] ("SDO") is an example of how these principles are applied in statutes in Hong Kong. The SDO expressly allows the court to grant "punitive or exemplary damages."[86] In *Yuen Sha Sha* v *Tse Chi Pan*,[87] the defendant sexually harassed the plaintiff contrary to the SDO. The court applied the relevant provision in the SDO and granted exemplary damages against the defendant to punish for his conduct in inflicting the harm. As for aggravated damages, although the SDO did not expressly authorise awarding aggravated damages, in view of the defendant's conduct after the event of sexual harassment, e.g. failing to make an apology until the last minute, prolonging the settlement of the matter, the court considered that his conduct further distressed the plaintiff and added insult to the injury. Therefore aggravated damages were awarded.

Both the rationale behind aggravated and exemplary damages show that the common law considers that the conduct of the defendant, in addition to the loss suffered by the plaintiff, is a relevant factor in determining the damages payable to the defendant. For exemplary damages, the fact that the Octopus case fits with the underlying rationale of the second category of cases identified in *Rookes* v *Barnard* in which exemplary damages should be awarded justifies the statutory authorisation of it. Given that the low amount of damages payable under the current regime and the fact that few data subjects will seek compensation from Octopus under the s66 mechanism, Octopus can profit from the breach. Exemplary damages can act as a proper deterrence and punishment against the data user and provide adequate remedies to balance the injustice caused by the current regime. As for aggravated damages, *Yuen Sha Sha* v *Tse Chi Pan* has demonstrated that statutory authorisation is not a pre-condition for the court to grant aggravated damages as remedies for a statutory wrong. In fact, the English court in the *Campbell* case has granted aggravated damages. The court held that the publication which

[83] [1998] QB 498.
[84] *Ibid.* at 512.
[85] Cap 480.
[86] Section 76(3A)(f).
[87] [1999] 1 HKC 731.

involved an unlawful disclosure of her personal data has trashed her as a person in a highly offensive and hurtful manner. An additional £1,000 was awarded. It seems that in cases which involve the transfer of non-intimate personal data in mass, as in the Octopus case, is unlikely to cause any special injury to feelings as in the *Campbell* case. Aggravated damages should nevertheless be included in the PDPO for two reasons. First, the Hong Kong courts have not yet made any precedents in granting aggravated damages in the PDPO cases. Yet the *Campbell* case demonstrates situation which shows that aggravated damages is necessary in some cases. Including aggravated damages in the PDPO provides a stronger statutory basis on which the court can exercise its discretion to award such damages in appropriate cases. Second, the distinction between aggravated and exemplary damages is often blurred. Including both types of damages guarantees that extra damages can be awarded in cases which the conduct of the defendant is reprehensible.

A potential problem associated with statutory authorisation of aggravated and exemplary damages is that it might encourage frivolous claim. However it is believed that risk is minimal as it is balanced by the difficulty in proving the damages. For exemplary damages, as stated in *Broome* v *Cassell*, unjust enrichment is a necessary but not a sufficient factor. The plaintiff has to demonstrate the defendant is subjectively aware the likelihood of making a profit out of the breach. As for aggravated damages, the plaintiff has to prove that the conduct of the defendant has aggravated his loss by injuring his dignity and pride. It thus seems that aggravated damages will only be granted in circumstances which the plaintiff has already suffered considerable loss. Therefore, it is believed that the statutory authorisation will have a stronger effect in deterrence than in encouraging litigation.

VI. Conclusion

The recent Octopus case shows that, with respect to cases which involve a mass collection of personal data and subsequent sale of the data, there are flaws in the PDPO which may frustrate the purpose of the legislation. Anonymous data has to be brought under the scope of the PDPO in order to prevent easy circumvention of the law and to protect data subjects from the same kind of harm which the law seeks to prevent. The amount and uniqueness of the data, and how intimate the data is related to the individual are all factors which should be considered when

determining whether the piece of data is included. With regards to the standard of protection, unnecessary terms in the PDPO and confusing test should be deleted and replaced. The no-consent model does not provide the right question for the court to consider. Emphasis should be placed whether the data subject has actually been informed. Consent of the data subject is an issue which should be brought back by presuming non-compliance of the PDPO unless prescribed consent is proved. The damages which can be claimed under this type of cases are exceptionally low and it causes injustice. Statutory authorisation of aggravated and exemplary damages is necessary to balance the injustice and provide proper deterrence to data users.

The solutions provided however are not intended to be able to solve all the problems associated with personal data. Personal data protection is a broad topic which does not only include data collection and subsequent transfer of them. Even the cases cited in this article indicated that there is a variety of situations which we can say there is an act of data collection falling within the scope of the PDPO. After all, the PDPO is a piece of legislation intended to cover a wide range of situations; yet it is almost impossible for the drafters to envisage all the situations and provide protection without losing the generality required. It is perhaps necessary to conduct a similar study every time when a new personal data issue arises in order to perfect the PDPO so that it can offer the adequate amount of protection.

Bibliography

Cases

Eastweek Publisher Ltd v *Privacy Commissioner for Personal Data* [2000] 1 HKC 692

Durant v *Financial Services Authority* [2003] EWCA Civ 1746

Shi Tao v *Privacy Commissioner for Personal Data* [2008] 1 HKC 287

Cinepoly Records Co Ltd & Ors v *Hong Kong Broadband Network Ltd & Ors* [2006] 1 HKC 433

Chan v *Privacy Commissioner for Personal Data* Administrative Appeal Board No. 4/1997

Campbell v *Mirror Group Newspapers* [2004] 2 AC 457

Tse Lai Yin Lily v *Incorporated Owners of Albert House* [1999] 1 HKC 386

Wing Lung Bank Ltd v *Privacy Commissioner for Personal Data* [2010] 6 HKC 266

Wong Wing Kit v *Octopus Holdings Limited & Octopus Rewards Limited* SCTC 36611/2010

Tam Yuen Hoi v *Chau Mu Cheng & Ors* [2003] HKCU 927

Royal Bank of Scotland plc v *Etridge (No 2)* [2002] 2 AC 773

Rookes v *Barnard* [1964] AC 1129

Broome v *Cassell* [1972] AC 1027

Appleton v *Garrett* [1996] PIQR P1

Thompson v *Commissioner of Police of the Metropolis* [1998] QB 498

Yuen Sha Sha v *Tse Chi Pan* [1999] 1 HKC 731

Legislation

Personal Data (Privacy) Ordinance (Cap 486)

Hong Kong Bill of Rights Ordinance (Cap 383)

Banking Ordinance (Cap 155)

Interpretation and General Clauses Ordinance (Cap 1)

Data Protection Act 1998

Control of Exemption Clauses Ordinance (Cap 71)

Sale of Goods Ordinance (Cap 26)

Construction Sites (Safety) Regulations (Cap 38A)

Sex Discrimination Ordinance (Cap 480)

Books

Stefan Lo, *the Annotated Ordinances of Hong Kong Personal Data (Privacy) Ordinance (Cap 486)* (LexisNexis 2006)

Mark Berthold and Raymond Wacks, *Hong Kong Data Privacy Law* (2nd edn Sweet & Maxwell 2003)

Abu Baker Munir & Siti Hajar Mhod Yasin, *Privacy and Data Protection* (Sweet & Maxwell 2002)

Rosemary Jay & Angus Hamilton, *Data Protection Law and Practice* (2nd edn Sweet & Maxwell 2003)

David K. Allen, *Damages in Tort* (Sweet & Maxwell 2000)

Ian McLeod, *Legal Theory* (3rd edn Palgrave MacMillan 2005)

Susan Singleton, *Tolley's Data Protection Handbook* (Butterworths Tolley 2001)

Heather Rowe, *Tolley's Data Protection Act 1998: a Practical Guide* (Tolley 2000)

Diane Rowland & Elizabeth Macdonald, *Information Technology Law* (3rd edn Cavendish 2005)

Peter Carey, *Blackstone's Guide to the Data Protection Act 1998* (Blackstone Press 1998)

Journal articles

Robin McLeish, 'Discovery and Data Protection' 31 HKLJ 49

Raymond Wacks, 'Privacy and Anonymity' 30 HKLJ 177

Alana Maurushat, 'Who Let the Cat out of the Bag? Internet Data Leakage and Its Implications for Privacy Law and Policy in Hong Kong' 39 HKLJ 7

Newspaper articles

The Standard, 'Octopus in hot water over "sold" personal data claim' 15th July 2010

The Standard, 'Cardholders file $50 Octopus claims' <http://www.thestandard.com.hk/news_details.asp?pp_cat-30&art_id=101430&sid=29163832&con_type=1> accessed 11th February 2011

Sun Daily, '獎賞公司洩私隱八達通擬覆核' (Octopus Reward Ltd leaked personal data, Octopus contemplating judicial review) <http://the-sun.on.cc/cnt/news/20101229/00412_003.html> accessed 11th February 2011

Other resources

Octopus Holdings Limited, ‘Our History’ <www.octopus.com.hk/about-us/corporate-proflie/our-history/en/index.html> accessed 11th February 2011

Octopus Holdings Limited, ‘Services in Hong Kong’ <www.octopus.com.hk/about-us/corporate-profile/services-in-hong-kong/en/index.html> accessed 11th February 2011

Office of the Privacy Commissioner for Personal Data, ‘The Collection and Use of Personal Data of Members under the Octopus Rewards Programme run by Octopus Rewards Limited’ Report Number: R10-9866

Octopus Holdings Limited, ‘How does it work?’ <www.octopus.com.hk/earn-and-redeem-rewards/how-does-it-work/en/index.html> accessed 11th February 2011

RTHK, ‘Legal fees warning in Octopus case’ <www.rthk.org.hk/rthk/news/englishnews/20100904/news_20100904_56_696075.htm> accessed 11th February 2011