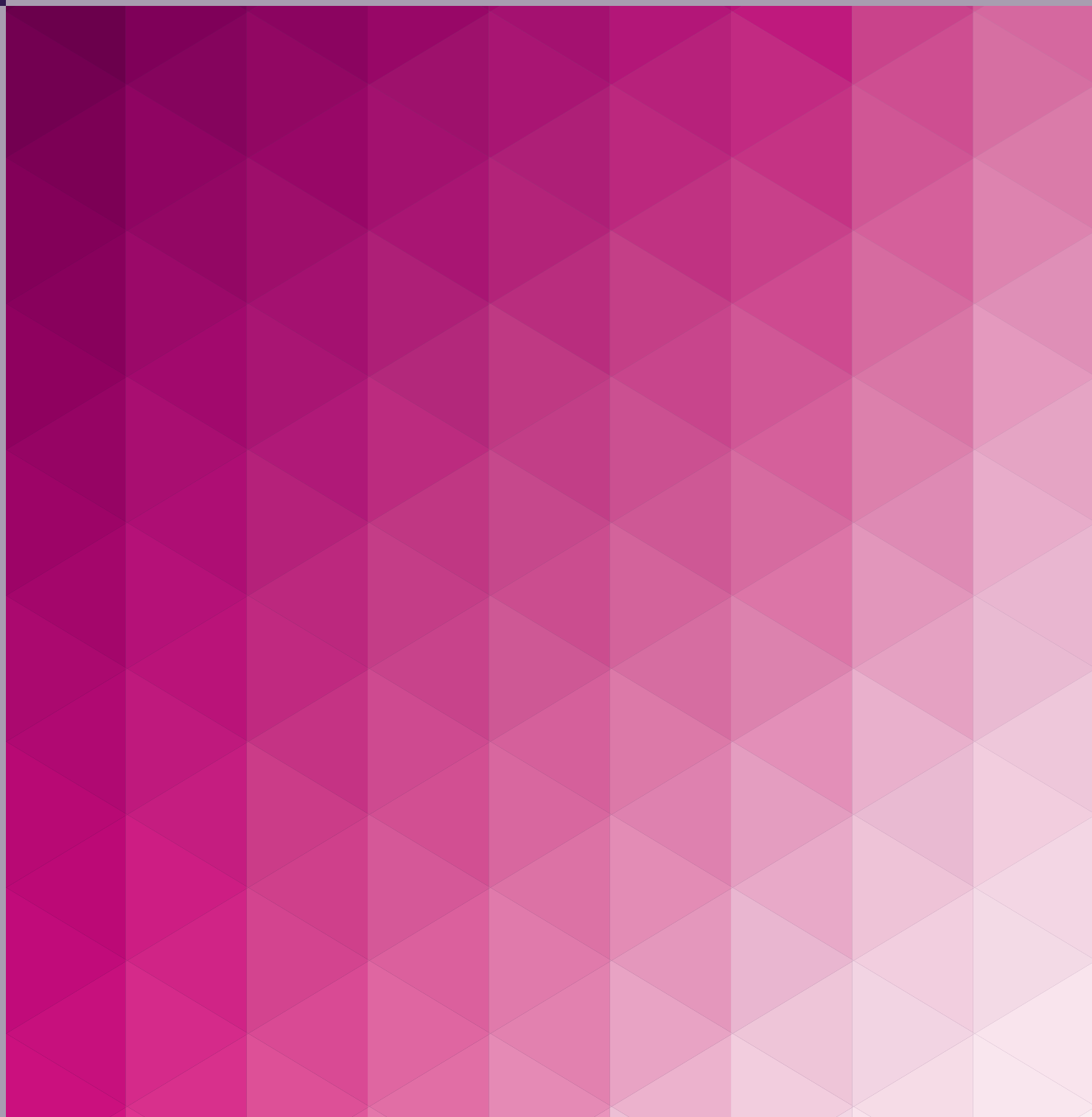
DEACONS
的近律師行

Status of Personal Data lawfully in the Public Domain



Contents

Introduction

There has been much debate over the Privacy Commission's intervention into the packaging-up (or 'aggregation') of personal data in the public domain, facilitating searches by members of the public of such data. This intervention focused on the 'Do No Evil' App operated by Brilliant United Investments Limited (**BUI**) and resulted in the Privacy Commissioner (**Commissioner**) serving an enforcement notice on Glorious Destiny Investment Limited (**GDI**) requiring it to cease supplying personal data to BUI for the purposes of the App. In addition, the Commissioner published a Report No. R.13-9744 into the App (**Report**) and issued a Guidance Note on the Use of Personal Data Obtained from the Public Domain in August 2013, shortly after taking the enforcement action. The Commissioner has also published several articles in the media attempting to justify his position.

In this article, I will examine the Commissioner's reasoning behind his decisions, comment on some rather surprising omissions and make some general observations about the use of personal data which are lawfully and officially in the public domain.

This article was originally written in the early part of 2014. Readers should note that it does not consider this year's controversy in Europe about the right to be forgotten nor does it comment on the Commissioner's recently issued Best Practice Guide for Mobile App Development (which can be found at this link: http://www.pcpd.org.hk/english/resources_centre/publications/guidance/files/Mobileapp_guide_e.pdf).

The 'Do No Evil' App

The Commissioner received 12 complaints from individuals about the App. Of these 12 complainants, four individuals were prepared to pursue their cases. Under section 38 of the Personal Data (Privacy) Ordinance (Cap. 486) (**PDPO**), the Commissioner is obliged to investigate a complaint to see whether the act complained of is in breach of the PDPO.

In addition, one of the functions of the Commissioner under section 8 of the PDPO is to 'monitor developments in ... the processing of data and information technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal data' - so the Commissioner would have been justified in looking into technologies such as the 'Do No Evil' App, even if he had not received any formal complaints.

The App (which was initially free but had to be paid for after the first few uses) enabled subscribers to search a data base compiled by GDI from information made public by the Judiciary, the Official Receiver's Office and the Companies Registry about current court actions (both civil and criminal), bankruptcy proceedings and Hong Kong company directorships. In other words, the data were officially and lawfully public. All of the data were (and still are) available to the general public from the individual sources but the App was a convenient way of putting the data under 'one roof' and facilitating searches against particular names.

The Commissioner's principal concern seemed to be the fact that the App made searching public registers convenient. It is worth quoting the Commissioner verbatim on his concerns:

> *'Members of the public have to spend a lot of time and effort if they wish to retrieve all the above mentioned information of the complainants from the Judiciary, Gazettes and the ORO or the relevant websites. However, any user of the App can access the above data simply by conducting a name search of the complainants via the App. If a user only intends to search the complainant's bankruptcy data, he may additionally learn that the complainant has been prosecuted for a criminal offence if he uses the App for the search instead of going to the ORO. This is obviously an intrusion to the privacy of the complainant'* [1].

[1] para 39, 18 of the Report

It is interesting to note that the Commissioner seems to think it is a 'good thing' that it takes a lot of time and effort for members of the public to search for information which is intended to be publicly available by the authorities. Surely, it should be the other way around. If the law requires information to be public, then it should be easy and convenient to find it. Further, it is not clear why learning that someone has been prosecuted for a criminal offence when searching for bankruptcy data is 'obviously' an intrusion into that person's privacy when the fact of that criminal offence is already a matter of public record.

He went on: '*Sensitive data of the data subject is disclosed without his knowledge and consent*' [2].

Yet, it is not clear that the data *are* disclosed without a data subject's consent. As will be seen below, the collection of the personal data by the agencies is generally not subject to any restriction on use and the data are published for the whole world to see. Further, data subjects also do not know who is searching for their data in the public registers - why it is a problem to search for the data using the App but not by searching the register direct is not explained.

In any event, the Commissioner's justified his enforcement action relying on two specific lines of argument, one based on the PDPO, namely the purposes for which personal data may be used under the PDPO as provided for in data protection principle 3 (**DPP3**)[3], and the other based on what he termed '*the reasonable expectation of the data subjects on the further use of their publicly disclosed data*' [4].

The 'Spirit of the Courts' and DPP3

Under DPP3, personal data shall not be used for any purpose other than the purpose for which the data were to be used at the time of the collection of the data or for a directly related purpose, without the consent of the individual who is the subject of the data. Although the personal data available via the App were sourced from public registers, the Commissioner argued that these data were still subject to DPP3 and therefore their use could still be limited. Generally speaking, this would appear to be the correct approach to take.

In the Report, the Commissioner examined the purposes for which personal data held in the various Government and Court public registers could be used.

The Commissioner was forced to admit that the Rules of the High Court do not specify any purposes for which searches of writs and judgments at the Registry of the High Court can be made, and no specific purposes of use of personal data are imposed when court proceedings are initiated by or against an individual. The only requirement is a fee to access the data[5]. In spite of this, the Commissioner concluded that the purposes for which searches could be made must relate to: '*the spirit of the courts to ensure that court hearings are administered in an open and fair manner*' [6].

It is not clear how this could amount to a restriction on use, particularly given his opinion that the purposes must include 'openness'. However, he concluded that the public: '*could <u>only</u> (my emphasis) use the proceeding numbers or court document filing dates as search criteria to retrieve the civil litigation information*' [7].

In his opinion, GDI's practice of aggregating proceeding numbers and court filing dates with information such as individual names involved in litigation was not in line with this purpose. Without the App, members of the public would be required to search all court records to find out whether a particular individual was involved in litigation.

With respect to the Commissioner, the purposes of use he attributed to the court data have no basis in law and he cites no authority for this interpretation.

[2] para 40, 18 of the Report
[3] paras 51 and 52, 22 of the Report
[4] para 53, 23 of the Report
[5] Order 63, Rule 4(1), Rules of the High Court (Cap 4A)
[6] para 60, 24 of the Report
[7] ibid

Does the Judiciary enforce restrictions on use of data?

The App also used data from Daily Cause Lists published by the Hong Kong Judiciary – both online and physically outside the Court – that provide hearing details including time, court number, names of judges, parties and their representatives and the nature of the hearing or offence (if a criminal action). The lists are prefaced by the following note:

> *'Daily Cause Lists are published to provide members of the public with information on the schedule of court hearings and related matters. They also facilitate court users (including witnesses, defendants' family members, etc.) to know which court they should attend. After the relevant hearing day, such lists serve no other purpose and will not be retained. No person accessing a Daily Cause List shall use any personal data contained therein for any purpose not related to the purposes set out above.'*

According to the Commissioner, making Cause List information available through the App did not conform to the restricted purposes for which information in Cause Lists can be used specified in the note. The Commissioner may be on firmer ground here. The note is clear that personal data should not be used for any other purpose. However, the Cause List information is also online and available to anyone with an internet connection and it's not clear whether, and how, the Judiciary can enforce the restriction. Indeed, I am not aware of any such action having ever been taken by the Judiciary.

The Commissioner criticised GDI for not having any means to monitor and control the use of the personal data obtained via the App notwithstanding that one of the conditions of the App's use is not to violate any law. But precisely the same criticism can be levelled at the Judiciary, and arguably there is a greater onus upon it to control the use of the data because it is the source. The Commissioner instead stated that:

> *'the use of personal data in the Daily Cause Lists and bankruptcy data from the ORO register is regulated by the Judiciary and the ORO respectively. Public access to the data is to a certain extent restricted to specific purposes, thus affording protection to the personal data of the data subjects from misuse'* [8].

However, it would seem that none of the relevant agencies regulates the use of personal data or protects data from misuse, beyond inserting some restrictive working in user notices which are not, nor can they be, enforced.

Bankruptcy Notices – Intended to be Widely Publicised

The Commissioner also admitted that the Bankruptcy Rules (Cap. 6A) do not state any purpose for which bankruptcy orders are published. Rule 78 of the Bankruptcy Rules states simply that: *'Where a bankruptcy order is made the Official Receiver shall forthwith send notice thereof to the Gazette and to such local newspaper or newspapers as he may think fit.'*

In other words, there is no restriction on purpose. The purpose of publishing the order is to ensure that the information is as widely known as possible. The bankruptcy notices published in the Gazette make the bald statement that the relevant individuals are bankrupt and that debts due to them should be paid to the trustee in bankruptcy – there is no limitation on the purposes of use of this information. Instead, the Commissioner relies on restrictions on searches of the Official Receiver's register via its own website which state that the register is maintained for the purposes of the bankruptcy case and that searches of the register should be confined to use for these purposes. Given this restriction, the Commissioner says searches of the Gazette should be limited to the same purposes, a highly unreasonable conclusion. Unless the Gazette notice contains the same restriction as the Official Receiver's website, persons searching only the Gazette cannot reasonably be expected also to know of the Official Receiver's website restriction.

[8] para 41, 19 of the Report

The restriction against publishing bankruptcy information is as disingenuous as the restriction in the Judiciary's Daily Cause Lists. There is no evidence that the Official Receiver has ever attempted to control the use of the personal data about bankrupt individuals and/or enforce restrictions on use. The Commissioner similarly failed to criticise the Official Receiver for this.

Companies Registry Purposes of Use

The Commissioner also refers to the Companies Registry's Electronic Search Services (specifically their Terms and Conditions). These clearly state that data collected from online Companies Registry searches cannot be re-sold nor copies made of data from which products may be derived for resale, without the consent of the Registry. The Terms and Conditions further provide that personal data cannot be used except for the stated purposes. These purposes are based on section 305(1A) of the Companies Ordinance (Cap. 32) and include ascertaining (i) whether the searcher is dealing with a company or its directors/officers in matters of or connected with any act, or in the administration, of the company and (ii) the particulars of the company or its directors/officers for the purposes of (i). It is rather difficult to understand how these purposes may apply in practice, although they are wide and appear to cover any act of the relevant company or matters connected with the company's affairs.

Indeed, it is not clear if use of the data via the App was in 'breach' of these purposes - the Commissioner did not provide any evidence in his Report. He simply said that the combination of the data from the Companies Registry with other data from the Courts was not consistent with the prescribed purposes and exceeded the reasonable expectation of the relevant individuals as to the use of their personal data.

The Commissioner also suggested – but did not make any firm finding – that there had been a breach of the provision prohibiting resale of data without consent. The App was free for the first few uses and thereafter required payment. Clearly, if a subscriber paid for a search of the Companies Registry via the App, GDI and BUI would be in breach of the Terms and Conditions.

In any event, just as with the Judiciary and the OR, there is no evidence that the Companies Registry has ever enforced its Terms and Conditions or sought to control the actual use of personal data collected from it.

A 'Reasonable Expectation of Privacy'?

The Commissioner's other ground for taking enforcement action was that allowing App users to conduct a name search of writs and judgments *'exceeds the reasonable expectation of litigants on the use of their personal data by the court'* [9].

However, the PDPO does not allow for a 'reasonable expectation' concept nor has there been any court decision in Hong Kong introducing it in relation to the PDPO. DPP3 speaks only of purposes for which data are collected and directly related purposes. Unfortunately, the Commissioner did not offer any justification for introducing the concept – he simply said, without quoting any authority that, if there was no stated purpose of use of the data, he:

> *'... may consider the underlying legal principles, statutory requirements and the reasonable expectation of the data subjects on the further use of their publicly disclosed data'* [10].

This is regrettable because, if the PDPO does indeed include a 'reasonable expectation of privacy', its introduction deserves to be properly legally justified.

[9] para 57, 24 of the Report
[10] para 53, 23 of the Report

It is possible that the Commissioner was borrowing the concept from the Australian Information Commissioner's Guidelines to Information Privacy Principles (and in particular Information Privacy Principles 10 and 11). The Commissioner may have found the reference to 'reasonable expectations' in *Data Privacy Law in Hong Kong*[11]. In this book, the authors argue that the Australian 'reasonable expectations' rule should apply where data are collected but no purpose of use is prescribed. Yet, it is difficult to see why or how this should be relevant to Hong Kong or the PDPO. The Australian Privacy Act 1988 and Principles 10 and 11 apply specifically to 'agencies' – basically, Australian public bodies and courts. Its rough equivalent, DPP3, applies to all data users in Hong Kong, not just public bodies. If the Commissioner wishes to introduce a 'reasonable expectation' concept into Hong Kong privacy law, he should, first, promulgate similar guidelines to the Australian Guidelines and, secondly, be consistent with the source and apply the concept to the various Hong Kong agencies' (the Judiciary, the Official Receiver's Office and the Companies Registry, among others) handling of personal data.

It is also possible that the Commissioner was influenced by the development of the tort of breach of confidence by English courts following the enactment of the Human Rights Act (**HRA**) in 1998. It is outside the scope of this article to consider breach of confidence in detail but it is worth noting a few points. First, the HRA has revolutionised English law on breach of confidence and effectively 'folded in' to the tort a right to a reasonable expectation of privacy based upon article 8 of the European Convention on Human Rights (**ECHR**). Other than the PDPO, there are two Hong Kong statutes that afford general privacy rights akin to those in the HRA. These are the Basic Law (Cap. 2101) which contains a right to privacy of communication (see article 30) - not quite the same as personal data privacy - and the Bill of Rights Ordinance (Cap. 383) (**BORO**). The BORO incorporates parts of the International Covenant on Civil and Political Rights into Hong Kong law and article 14 of the BORO protects against arbitrary or unlawful interference with privacy. Like article 8 of the ECHR (which binds public authorities), article 14 only binds the Hong Kong Government, not private persons. However, the courts in England felt able to extend the application of article 8 to private individuals because of section 6 of the HRA which makes it unlawful for public authorities (which include the courts) to act in a way which is incompatible with a right under the ECHR (including article 8). There is no equivalent of section 6 in the BORO so it is unclear whether the Hong Kong courts would have a legal basis for applying article 14 in private civil claims in the same way as the English courts which are bound by section 6. Even if, as some English judges have suggested[13], section 6 of the HRA is not needed in order for the article 8 privacy right to apply as against private entities as well as public authorities, a claim for breach of confidence based on reasonable expectation of privacy is a common law right which has nothing to do with the PDPO.

Further, even if the concept of 'reasonable expectation of privacy' existed in Hong Kong law (which, it is submitted, is very doubtful), once personal data are lawfully and officially in the public domain, individuals can have no reasonable or realistic expectation of any restrictions on their use. The inability, not to say failure, of the Judiciary and other agencies to control use of personal data they have (lawfully) published is a stark illustration of this reality.

The Commissioner is therefore, in my view, wrong to rely on this concept as a ground for taking enforcement action against the App under the PDPO.

[11]Mark Berthold and Professor Raymond Wacks, FT Law and Tax, 1997
[12]ibid [127]
[13]eg Campbell v MGN Ltd [2004] UKHL 22 [18] (Lord Nicholls of Birkenhead)

Data aggregation

As has been seen, the Commissioner's main objection to the App was the fact that it *aggregated* a lot of personal data that had been made public by government agencies, making it very convenient to search against individual names using one convenient private source, rather than having to go to each agency to obtain the data separately. Further, it was clear that GDI was using considerable computing power in order to make the data available via the App. It is interesting to note that the PDPO already contains provisions dealing with mass processing of personal data to produce more data which may be used to take 'adverse action' against an individual. These are the 'matching procedure' provisions of the PDPO[14]. However, the Commissioner did not seek to rely on these provisions in justifying his enforcement notice. Indeed, he did not once mention matching procedures in the Report.

It is a shame the Commissioner did not take the trouble to consider whether GDI was conducting matching procedures as these provisions are the only ones in the PDPO which deal directly with mass processing of personal data – which is what GDI was doing. Given this omission, it is worth considering this question further.

Matching procedures can only be carried out (a) with the consent of the individual whose personal data are the subject of the procedure, (b) if the Privacy Commissioner consents, (c) if the procedure belongs to a specified class or (d) if it is required or permitted pursuant to a specified Ordinance[15]. Currently, no class of matching procedure or Ordinance has been so specified. There is also a relaxation of the strict rules if compliance with them would prejudice a criminal investigation[16]. Matching procedures are not subject to any exemptions under the PDPO. Carrying out a matching procedure in breach of the PDPO renders a person liable to a fine of HK$10,000[17]. It is therefore worth considering whether (i) GDI's data base or (ii) use of the App amounted to a matching procedure. For this purpose, relevant definitions from the PDPO[18] are set out below in full:

matching procedure means any procedure whereby personal data collected for 1 or more purposes in respect of 10 or more data subjects is compared (except by manual means) with personal data collected for any other purpose in respect of those data subjects where the comparison -

a) is (whether in whole or in part) for the purpose of producing or verifying data that; or

b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data,

may be used (whether immediately or at any subsequent time) for the purpose of taking adverse action against

any of those data subjects;

adverse action, in relation to an individual, means any action that may adversely affect the individual's rights, benefits, privileges, obligations or interests (including legitimate expectations).

Although GDI was collecting a large amount of personal data about more than 10 individuals from the relevant agencies and loading the data onto its data base, it only carried out a comparison procedure if it received a request via the App in relation to an individual's name. Provided it did not carry out this procedure at any one time in respect of more than 9 names, it would seem that it was not in breach of the matching procedure provisions. Comparisons of 10 or more individuals' names, though, would be likely to constitute a breach because it is quite likely that the results of the comparison procedures would be used for the purpose of taking action which may adversely affect the relevant persons' rights.

[14] ss 30 - 32
[15] s 30(1)
[16] s 31(6)
[17] s 64A
[18] s 2(1)

There is no evidence that either the App or GDI's data base was used to compare more than 9 persons' personal data at any one time. However, if it had been, then the Commissioner could have justified his action against GDI on the ground that it was carrying out unlawful matching procedures.

The important point to note from the above is that the PDPO already contains detailed provisions which regulate mass processing of personal data or data aggregation. It seems very clear that these provisions did not apply to the App.

Two exemptions that should have been considered

The Commissioner referred to certain exemptions provided by the PDPO which balance the conflict between privacy rights and the public interest[19] but concluded that none applied. However, he did not mention the exemptions under sections 51A or 60B of the PDPO.

Section 51A provides a blanket exemption from all data protection principles (including DPP3) in relation to personal data held by a court in the course of performing judicial functions. Section 51A does not say who can rely on the exemption and, surely, if the intention had been to limit the exemption to the use of personal data by the courts, it would have said so expressly. Further, if courts' use of personal data is unrestricted, should not that effect be transferred to any subsequent use of the same data if lawfully published? It is arguable, therefore, that this exemption can be applied to the App.

Section 60B provides that personal data are exempt from DPP3 if the use of the data is (i) required or authorised by or under any enactment, or pursuant to the law or any court order or (ii) required in connection with any legal proceedings. It must also be arguable then, that as the use of the personal data in question was so required/authorised pursuant to the Rules of the High Court, the Bankruptcy Rules, the Companies Ordinance and in connection with legal proceedings, DPP3 does not apply either to the publication of the data by the relevant Government agency or to any subsequent use.

The Commissioner's omission to consider the applicability of sections 51A and 60B to these circumstances is serious and must call into question his ultimate conclusion.

Conclusions and Observations

1. The Commissioner failed to make a case that the App does not satisfy the two main legal standards that he set for it. First, the uses of the information made public that he identified were not sufficiently restricted to prevent GDI and/or BUI from also making it available to the public. Secondly, even if there is a 'reasonable expectation of privacy' under Hong Kong law, (i) it is not a right afforded by the PDPO and (ii) individuals can have no reasonable expectation that use of information made public by any of these agencies will be limited or that the relevant agencies will or can take any action to control that usage.
2. Whilst the Commissioner sanctioned GDI and BUI for failing to monitor and control the use of the personal data obtained via the App, he did not sanction the agencies for failing to do so themselves. This is arguably a worse transgression because it is the agencies which make personal data public and purport to restrict the purposes of use of the data.

- The Commissioner made much of the possibility of confusing people with similar names (in his comments in the Report about searches against the name 'Chan Tai-man'[20]). However, these criticisms could more meaningfully have been directed at the sources of the data. The same problems arise if a search is made of the records of the Judiciary, the OR or the Gazette.

[19] para 80, 31 of the Report

- The Commissioner pointed out that data about court proceedings disclosed via the App may not always show the outcome of the proceedings – so, occasionally, an acquittal may not be disclosed. But direct searches of the Judiciary's records would produce exactly the same result– the Commissioner reserved his ire for the App though, not the Judiciary which was the source of the data.
- As has been seen, the Commissioner complained that individuals cannot know who has had access to their 'sensitive' personal information. Yet the information cannot sensibly be called sensitive as it has already lawfully and officially been made publicly available by Government agencies. Further, individuals also don't know who has accessed their data directly from the Government agencies.

3. A better approach would have been to accept that once personal data are lawfully placed in the public domain by any Government agencies, their use should be unrestricted. It is intellectually dishonest to argue that restrictions (to the extent that there are any) on use of personal data which have been made public by a Government agency should apply when it is very clear that the agency cannot control actual use of the data, and indeed has no intention of doing so. Having accepted this reality, the Commissioner should have considered whether other provisions of the PDPO applied to the App. (The Commissioner did make a start at this in his Report when he considered data protection principle 1(2) relating to the fairness and lawfulness of collecting the data from the agencies[21]. He concluded that collection by GDI was lawful and fair. Regrettably, he stopped there and did not consider whether the App breached any other data protection principles other than DPP3 or whether processing the data for publication via the App amounted to a matching procedure.) In my view, he could have set the following tests for the App, all based on the PDPO's data protection principles:

   a) Does GDI ensure that the personal data on its data base are accurate and, if inaccurate, does it erase the data? Does GDI ensure that personal data are not kept longer than necessary? These requirements of data protection principle 2 (**DPP2**) are relevant to GDI's treatment of personal data.

      The Commissioner referred to the Rehabilitation of Offenders Ordinance (Cap. 297)[22] which provides that an offender sentenced to imprisonment for less than 3 months or to a fine of less than HK$10,000 will be deemed not to have been convicted after three years have elapsed without another conviction. DPP2 would therefore require GDI to ensure that information about offenders who are not re-convicted within three years is removed from its data base.

      The Commissioner would have been well within his rights to enforce compliance with DPP2, but he did not even mention it.

   b) Did BUI advise App subscribers of the purposes for which search results could be used to ensure that these purposes mirrored the agencies' purposes? The Commissioner could have directed BUI to ensure that the purposes for which the data could be used were the same as any agencies' purposes.

   c) Does GDI protect its data base against unauthorised access under data protection principle 4?

   d) Does GDI allow individuals to ascertain whether it holds their personal data and that they can have access to the data and to correct them under data protection principle 6?

[20]paras 18 and 43-44, 7, 20 of the Report
[21]para 34, 17 of the Report
[22]paras 47 – 48, 21 of the Report

Access to Data: The Haves and Have Nots

There are several companies providing services in Hong Kong whose business involves aggregating public information and making it conveniently available, just as GDI and BUI were doing. These companies' services are used by banks, other financial institutions, law firms and accountants to conduct due diligence into individuals and companies. Their services have become essential for legally required anti-money laundering checks and for performing standard due diligence exercises and credit checks.

- Does the Commissioner's ruling against GDI and the App mean that these other companies cannot now aggregate public personal data as they have been doing for many years?
- If not, is it fair that financial institutions and businesses can have access to aggregated public personal data but the 'man in the street' not? The App is initially available free but is otherwise inexpensive. Is there an element of discrimination in the Commissioner's ruling? It could be interpreted as saying that businesses can have access to these data, but not the common man.

Conclusion

With respect to the Commissioner, he did not make out a satisfactory case that the service provided by the App either (1) was an infringement of personal privacy or (2) contravened the law.

If there is a public concern that use of personal data lawfully made public by Government agencies should be restricted or otherwise controlled, then the Commissioner should lobby for appropriate legislation which expressly addresses the point. The current law in Hong Kong does not attempt to protect such data (except perhaps in relation to company directors and information obtained from the Companies Registry).

The Commissioner should reconsider his position. Whilst I have no doubt that he reached his conclusions with the best of intentions, they may have far reaching and unintended consequences, including for Hong Kong's position as a business and financial centre, its culture of *laissez-faire* and its reputation for producing innovative services. Personal data lawfully put into the public domain by public bodies and agencies should be treated as public and freely available and the Commissioner should focus his attentions on more egregious abuses of personal data privacy.

Want to know more?

Simon Deane
simon.deane@deacons.com.hk
+852 2825 9209

DEACONS
的近律師行

5th Floor, Alexandra House
18 Chater Road Central
Hong Kong

Tel +852 2825 9211
Fax +852 2810 0431
E-mail hongkong@deacons.com.hk

www.deacons.com.hk