Drawing the Line: Differentiating between Access to Public Domain Information and Protection of Personal Data

Mr Allan Chiang, Privacy Commissioner for Personal Data

Myth

Many people are under the belief that personal data collected from the public domain, not from the data subjects direct, is open to unrestricted use. This is not correct.

Examples of sources of public domain information include:

Sources of public domain information	Types of personal data
Companies Register (as shown in annual returns and other prescribed forms)	• Names of directors and secretaries • Hong Kong Identity Card numbers ("HKID") or Passport numbers of directors and secretaries • Residential addresses of directors and secretaries • Email addresses of directors and secretaries (on voluntary basis)
Notice of Intended Marriage	• Names of bridegroom and bride • Marital conditions of bridegroom and bride • Dates of birth of bridegroom and bride • Residential addresses of bridegroom and bride (street name and district only)
Register of Electors	• Names of voters • Addresses of voters •

Professional registers (e.g. Solicitors' list/ Barristers' list)	• Names of members • Addresses of members • Sometimes, when and where professional qualification obtained • Contact information, e.g. telephone numbers, fax numbers and email addresses of members • Licensing condition, if any, imposed

Some people have said that there is no "copyright" in public domain information. Others have misguidedly argued that since the data is out in the open, it is no longer "secret" and hence warrants no protection. But keeping data confidential or observing the duty of confidence is not exactly the same as protecting personal data. The former is a duty based on contractual or fiduciary relationships. The latter is a manifestation of the fundamental right to privacy protected under the Basic Law.

Public domain personal data protected under the law

Personal data, be it publicly available or not, is subject to protection under the Personal Data (Privacy) Ordinance (the "Ordinance").

Prior to the enactment of the Ordinance in 1995, the Law Reform Commission had carefully deliberated on whether public registers should be exempted completely from the Ordinance and concluded that it should not. In the public consultation exercises leading to the latest amendments to the Ordinance (effective 1 October 2012 and 1 April 2013), the Government reaffirmed the view that "putting personal data in the public domain does not make the data available for use for any purpose". This was upheld in a Court of Appeal judgment delivered in February this year (*Re Hui Kee Chun*, CACV 4/2012).

Imagine the consequences if the opposite view was true. First, data users may get around the law by deliberately publicising the data in the public domain. Further, improper use of personal data which had been accidentally leaked to the public domain would be legitimised.

Privacy risks

At the very least, personal data in the public domain, if used and re-used indiscriminately and without appropriate safeguards, would result in loss of control over the accuracy, retention and security of the data, thus jeopardizing the interests of the data subjects.

The situation is aggravated by technological advances which support aggregation, matching and further processing of data in the public domain. Data of an individual collected from one public source could be combined with data of the same individual obtained from other public sources at phenomenal ease and efficiency to profile the individual and generate new uses of the data beyond the purposes for which they were initially collected.

Admittedly, profiling and re-use of the personal data in the public domain could generate immense economic efficiency and societal benefits. At the same time, such activities also pose grave privacy risks.

Example 1

A common example of these privacy risks is the use of personal data for targeting customers in marketing of goods and services. The US retail giant Target analyses the purchasing habits of its customers and is able to predict reliably whether a female customer is pregnant and by how many months. It caused great embarrassment when the father of a teenage girl found out that she was three months pregnant following suspicions about the increased amount of pregnancy-related advertisements from Target arriving in the mail. That Target has "data-mined" its way into the customer's womb is clearly privacy-intrusive.

It is conceivable that many marketers are using innovative analytics to enhance marketing effectiveness based on customer-supplied data and public domain data. The problem is not so much related to the nature and source of the data but rather to the way the data is combined, further processed and used.

Example 2

Another example is the compilation of bankruptcy and litigation records of individuals by certain data brokers based on the Judiciary's daily cause lists and cause books as well as the bankruptcy order notices in the Government gazette.

This is the subject of our recent investigation into a smartphone application which enabled subscribers to search such records by name and view the combined data in one go. The data subjects concerned could be harmed unknowingly if the data is used, for example, for checking their employability or credit-worthiness.

Firstly, as different persons can share the same name or have similar names, it is problematic to ascribe the data to a target individual according to his name. Secondly, a person involved in litigation could be perfectly innocent but the database did not as a rule include the court's decision in his favour. Thirdly, bankruptcy is normally discharged after four to eight years, while the Rehabilitation of Offenders Ordinance prevents unauthorised disclosure of a previous minor conviction, provided the offender has not been reconvicted for three years. Retention and use of the bankruptcy and litigation data indefinitely would therefore unduly stigmatise the individual and bar him from leading a normal life free from encumbrances.

Example 3

A further example is the unfettered access to information sources like the companies, land, and vehicles registers, which puts sensitive data such as HKIDs, full residential addresses and signatures at stake. If the data was exploited by persons with malicious intent, the data subject would suffer the risks of financial loss, identity theft and personal safety (through stalking and surveillance).

For this reason, we recently secured the cooperation of a website operator to cease operating a HKID index whereby names of individuals and their HKIDs found in the public domain were listed together to enable search by either name or HKID. Such aggregation and processing of sensitive personal data were clearly inappropriate.

This website operation must be distinguished from that of a search engine which acts purely as an intermediary in providing content data. Without performing value-added operations on the personal data it processes, aggravation of privacy risks does not come into question.

Use limitation principle

The most relevant provision in the Ordinance which regulates the use of personal data in the public domain is Data Protection Principle 3 ("DPP3"). This is a use limitation principle which provides that personal data should only be used for the purposes for which it was collected or a directly related purpose, unless the explicit and voluntary consent of the data subject is obtained.

The starting point for an application of DPP3 is thus the original purpose of collecting the personal data and making it publicly available. Public registers are normally set up by statutes. Ideally, the purpose of a public register should be stated as specifically as practicable in the enabling legislation.

An example of such specific statement of purpose is found in Section 136 of the Securities and Futures Ordinance which states that the Securities and Futures Commission's register of licensed persons and registered institutions is maintained "for the purposes of enabling any member of the public to ascertain whether he is dealing with a licensed person or a registered institution in matters of or connected with any regulated activity and to ascertain the particulars of the licence or registration of such person or institution (as the case may be) … "

Where the purpose of a public register is not expressly stated in the legislation, it could be implied. Very often, one can find the purposes and limitations of use of the public domain information spelt out at the user interface.

For example, the Register of Vehicles is established under the Road Traffic (Registration and Licensing of Vehicles) Regulations "to provide for the regulation of road traffic and the use of vehicles and roads (including private roads) and for other purposes connected therewith." Hence the permitted use of personal data should relate to traffic and transport matters.

Similarly, the permitted use of the personal data in the Notice of Intended Marriage should be to enable any person authorised by law to object to the proposed marriage. Also, professional or business directories must have been created to enable clients, actual or potential, to approach the listed persons in their professional capacities.

In a similar vein, the Government telephone directory incorporates an explicit use restriction to the effect that the government officials' names and contact details listed are provided to facilitate official communication between the Government and the public, and not intended to be used for direct marketing activities, or transfer for commercial gains.

Having ascertained the original purpose of collecting the personal data and making it publicly available, the question of whether the re-use of such data is for the same purpose or a directly-related purpose has to be assessed on a case-by-case basis.

We need to explore the specific context in which the data was collected and the reasonable expectations of the data subjects as to the further use made of the data based on that context. The test here is whether a reasonable person in the data subject's situation would find the re-use of the data unexpected, inappropriate or otherwise objectionable, taking into account the sensitivity of the data and the context of the data collection. The three examples of privacy risks mentioned above serve to illustrate this test.

Exemptions

The right of individuals to privacy is not absolute. It must be balanced against other rights and public interests. Accordingly, the Ordinance specifically provides for certain exemptions from the application of DPP3 and they apply equally to personal data in the public domain.

These exemptions cover a wide range of areas. In particular, Section 58 caters for personal data used for the prevention or detection of crime or for the prevention, preclusion or remedying of unlawful or serious improper conduct or dishonesty or malpractice by persons. This may be relevant for data users engaged in law enforcement and professional due diligence. Also, Section 61 provides for the exemption from DPP3 for news activity where the publishing

or broadcasting of the personal data is in the public interest. For lawyers, it is important to note that Section 60B provides for exemption where the use of the data is required or authorised by or under law, by court orders, or required in connection with any legal proceedings in Hong Kong or for establishing, exercising or defending legal rights.

Administrative and technological safeguards

It is meaningful to take stock of the administrative and technological measures that have been taken to guard against improper use of the personal data in the public domain. The following is a snapshot in relation to those data held by the Government.

In the case of the Register of Vehicles, the Transport Department in 2003 introduced some administrative measures to remind applicants for vehicle owners' particulars that all information provided should be used for traffic and transport related matters, and that they may commit an offence if they knowingly make a false statement in the application.

In the case of the Land Register, procedural safeguards are in place to prevent massive downloads of data made available online.

To the credit of the Marriage Registry, the Notice of Intended Marriage was amended in 2005 so that only part of the personal data supplied by the marrying parties has to be exhibited. HKIDs, full details of the residential address and names of the parents need not be disclosed.

As regards the Register of Electors, again massive download of data by the public is not possible, albeit relevant voters' particulars are supplied to the election candidates under prescribed conditions. Further, legislative sanctions against unlawful use of voters' personal data kept in the register are in place. The use of such data other than a purpose related to the election is an offence under the relevant Electoral Affairs Commission Regulations which attracts a fine at Level 2 and imprisonment for six months.

Further, as indicated above, the Government telephone directory incorporates an explicit use restriction to the effect that the government officials' names and contact details listed are not intended to be used for direct marketing activities

and the information should not be transferred for commercial gains. Although this use restriction clause does not have the force of law as the Electoral Affairs Commission Regulations in the previous example, it is a recommended best practice for all business or professional directories.

There is a long way to go for data users to measure up to the data protection standards enshrined in the Ordinance enacted 18 years ago.

In the vehicles register case, despite the administrative measures implemented by the Transport Department, abusive use of owners' data is still possible. The main reason is that even if the applicant for data fails to specify the purpose of the application or states whatever purpose, the Commissioner for Transport has no discretion to decline to release the data requested. Against this background, the Government in 2011 proposed to amend the legislation to ensure the proper protection of vehicle owners' personal data. However, there is little progress on this front.

Meanwhile, the new Companies Ordinance enacted on 10 August 2012 has incorporated a provision to the effect that the full identification numbers and residential addresses of company directors will not be made available on the register for public inspection. However, it is disappointing that the Government has decided in March 2013 to defer consideration of implementing this particular provision following some belated expression of reservation by some stakeholders.

Equally disappointing was the Government re-affirming in February 2013 that it has no immediate plan to amend the relevant legislation to afford protection of property owners' personal data through imposing restrictions in the search of land registers and copies of registered instruments. Presumably there will be a breakthrough when the present deeds registration system for recording land and property transactions is converted to a title registration system through the commencement of the Land Titles Ordinance, which was enacted in July 2004. When this will happen is anybody's guess.

Conclusion

The present state of affairs is far from satisfactory. The pace of legislative reform to enhance data protection is dictated by the Government and the legislators. On our part, we will strive to make an improvement through public education, enforcement and engagement with stakeholders.