Private sector uses of 'public domain' personal data in Asia: What's public may still be private

Author: Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2014) 127 *Privacy Laws & Business International Report*, 13-15

Some data privacy laws, particularly those outside Europe, have very wide exemptions from their data privacy legislation for personal data which is 'publicly available' in some way. Such information is often conveniently, but erroneously, called 'public domain' data. However, in Asian jurisdictions these exemptions vary a great deal in their scope. More important, in some jurisdictions, there are no such exemptions at all. This variation poses a considerable risk to any businesses or NGOs that intend to re-use personal data that is somehow 'publicly available' from one or more Asian jurisdictions. These dangers were most clearly illustrated by a business that was in effect forced to close by Hong Kong's data privacy law.

The 'Do No Evil' app in Hong Kong

Hong Kong's *Personal Data (Privacy) Ordinance* has no explicit exemption for publicly available information. A recent ruling by Hong Kong's Privacy Commissioner[1] makes it clear that such data is not in the 'public domain' (in the sense that anyone can do what they like with it). GDI is a Virgin Islands company registered in Hong Kong as an overseas company. 'Its main business is to collate publicly available litigation, bankruptcy and company directors' data for compiling a database for access by its customers including professionals in the legal and accounting industries to perform due diligence/background reviews on target persons.'[2] It planned to expand its business to smartphone users in Hong Kong, in partnership with Hong Kong company BUI which built the application for smartphones (app) named 'Do No Evil' (DNE app). The DNE app accessed a database compiled and controlled by GDI. The DNE app was launched in February 2012 as a free download, but with paid access to the database. Within fifteen months there were 40,000 downloads and 200,000 accesses to the database. The Commissioner held that GDI was the 'data user' with obligations under the Ordinance. In August 2013, in light of the Commissioner's decision, the company stopped providing the DNE service.[3]

The database accessed by the DNE app contained the following information from public registers and websites provided by Hong Kong public authorities: (i) Daily cause lists; (ii) Judgments (full text); (iii) Cause books, including information from originating process documents; (iv) Writ of summons, some including statements of claim; (v) Gazette, including date of declaration of bankruptcy and discharge; and (vi) Annual returns of companies, including directors (and shareholders of limited companies). All of (i)-(vi) included the names of the various parties, and their addresses in almost all. Cause numbers were given in (i)-(iv), and, partial HK ID numbers in (v), and full ID numbers in (vi). The key feature of the DNE app was that it allowed all of these sources to be searched simultaneously by a person's name, or part of their name, or other data.

---

[1] Privacy Commissioner for Personal Data 'Glorious Destiny Investments Limited and Brilliant United Investments Limited Publicly Disclosed Litigation and Bankruptcy Information Collected from the Public Domain to Their Customers via Smartphone Application "Do No Evil"' (Investigation Report under Section 48(2), R13-9744, 13 August 2013) <www.pcpd.org.hk/english/publications/files/R13_9744_e.pdf >; See also the Privacy Commissioner's Press Release at <http://www.pcpd.org.hk/english/infocentre/press_20130813.htm>

[2] Section 48(2) Report, p4

[3] See DNE website <http://www.donoevil.hk/pc.html> and the company's statement (behind the iPhone icon).

'A myriad of privacy concerns'

The Commissioner first discussed six of what he described as 'a myriad of privacy concerns', before considering whether GDI had breached the Ordinance. The following is a very brief summary of a lengthy discussion, and indicates some of the policy justifications for this type of law:

(i) The DNE App involved use of 'sensitive personal data'. This was mentioned by the Commissioner as a privacy concern, but Hong Kong's Ordinance does not have any special rules concerning sensitive data which can lead to breaches.

(ii) The aggregation of data otherwise scattered across different registries could be much more intrusive and damaging to an individual. For example, a user looking for bankruptcy information may find information about unrelated criminal charges.

(iii) Data subject have no means of knowing that their personal data has been accessed (or, we could add, who has accessed it). This bypasses legislation in Hong Kong such as that which informs job applicants if a sexual convictions record check will be done.

(iv) Some of the registers concerned impose limits on further use of the information, whereas no limits are imposed on those who use the DNE app. 'Indiscriminate' access may result in data subjects' losing 'opportunities for employment, education, making friends and credit applications'.

(v) The data accessible by the DNE app 'is not accurate, up-to-date or comprehensive.' The Commissioner illustrated this by a search for a hypothetical named individual, describing how users might reach erroneous conclusions about a person with such a name. GDI did operated a 'Redress File' facility, whereby data subjects who became aware of prejudice because of misleading or incomplete information could (supposedly) add information to GDI's records. He considered this shift of responsibility was unfair.

(vi) The DNE app jeopardised offender's chances of rehabilitation by providing information in ways that 'definitely defeats the legislative intent of the Rehabilitation of Offenders Ordinance'.

Contraventions of the Ordinance

None of the above privacy concerns constituted, in themselves, breaches of the Ordinance. The Commissioner, paraphrasing Data Privacy Principle 3 (DPP 3),[4] put the legal issue as follows:

> Personal data, be it made publicly available or not, is subject to protection under the Ordinance. DPP3 provides that personal data should not be used for any purpose other than the original purpose for which the data was to be used at the time of collection or a directly related purpose, unless the prescribed consent of the data subject is obtained.

Concerning 'purpose', the Commissioner stressed that it was not GDI's purpose of collection that was of primary importance, but the purpose for which the government bodies concerned made the data available:

> … the original purpose or directly related purpose refers to the original purpose of making the complainants' data publicly available by the Judiciary, the Companies Registry and the ORO, instead of the purpose of collection of such data by GDI from the public domain. A public register is usually established for a stated purpose which is either explicit or can be implied from the enabling legislation. The purpose of use of the personal data therein is stated in the relevant legislation, either explicitly or implicitly. In both cases, data users should only use the data for the stated purposes, or in accordance with the purpose of the public register, or a directly related purpose.

[4] DPP 3 states: 'Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than – (a) the purpose for which the data were to be used at the time of the collection of the data; or (b) a purpose directly related to the purpose referred to in paragraph (a).'

The Commissioner therefore first considered the purposes stated on each of the websites or office systems from which information was extracted by GDI, then if necessary the provisions of the relevant Ordinances under which they operate (and the general purposes of the justice system). In each case, he found that the uses which the DNE app allowed (and aimed at providing) went considerably beyond anything that was an express or implied purpose of the websites or Ordinances (and in some cases expressly contrary to them).

Comment – The (ir)relevance of the data subject's expectations

The Commissioner then needed to consider whether the DNE app might still constitute a 'directly related purpose'. He seems to have done so by first considering first whether the relevant registry or Judiciary would reasonably expect the information to be used as the DNE app used it, and he did not find this so in any case, basically because of the indiscriminate way in which the information was distributed. Second, he then considered what would have been 'the reasonable expectation of the data subject' in each case, and he similarly found that data subjects would not have reasonably expected what the DNE app did with their personal data. It is arguable that this second step is unnecessary here, because in all or almost all cases, information in public registries is provided under compulsion, or results from court proceedings. Where personal data is provided voluntarily, user expectations could be relevant to what are 'directly related purposes' for which registries provide the data to the public, but their relevance is questionable when the data is gathered by compulsion and data subjects can reasonably presume that it will only be used by third parties consistently with the statutory purposes. The data subject's expectations made no difference in this instance, and would rarely do so where compulsorily collected information is involved.

Controversy but no appeal

GDI did not appeal to the Administrative Appeals Board, so there is no further resolution of the matter beyond the Commissioner's decision. Any businesses within the reach of Hong Kong's law who attempt to aggregate public registry data can expect that, unless they comply with the approach set out in Commissioner Chiang's s 48(2) Report, they may face a complaint and a similar result. There were some adverse reactions to the decision, such as from the Wireless Technology Industry Association, but they were based on rejection of the policy of the Ordinance.

Potential dangers in the DNE app decision

Potential dangers in the DNE app decision need to be considered. It is not a danger to freedom of speech, and particularly to the media, because the Hong Kong data privacy Ordinance has robust exceptions in favour of the media, which are likely to allow journalists to utilise public registers for investigate reporting, and there are constitutional protections of free speech.

Another danger is that the Hong Kong administration could misuse the decision by placing unjustifiably restrictive conditions of re-use on public registers (although consistent with the enabling Ordinances). In some cases, copyright law could be used to impose similarly unjustified restrictions, because Hong Kong has 'Crown copyright'. The real problem here is that Hong Kong does not have any 're-use of public sector information' laws which give any guarantees of re-use being allowed. It is reasonable for the technology sector in Hong Kong (or NGOs wanting to increase transparency of government and business operations) to want to ensure that the Ordinance is not misused to stifle innovation, creative re-use of government information and transparency. But it is not the answer to abandon the privacy of data subjects to indiscriminate and ill-managed republication simply because a name similar to theirs appears in a public register. In all jurisdictions, privacy protection of public register information is reasonable public policy, but it needs to be matched with good policy to prevent abuse.

Where else in Asia can you Do No Evil?

There are a wide range of positions being taken on this question, in Asia and elsewhere. A comprehensive account for the nine other jurisdictions in Asia with data privacy laws cannot be given here, but the general position in each – and some of the uncertainties – can be indicated.

Hong Kong takes the more privacy-protective position, similar to **European** law, which does not provide any general exemption for publicly available information, but does allow specific exemptions to be made for public registries containing personal data, and relaxes the special protections for sensitive data which have been 'manifestly made public by the data subject'.[5] Hong Kong similarly allows each public register to set its own conditions for use of the information in it.

Like Hong Kong, the laws in **Macau** and **South Korea** contain no explicit exclusion from protection of publicly available information. However, like Hong Kong, they do provide countervailing protections for freedom of speech (and thus journalism), either through constitutional protections or through specific provisions in their data privacy laws, or through both. These free speech protections are not complete exemptions, and in a case like that of the Hong Kong DNE app, the result would be likely to be similar.

Japan has no exemption for publicly available information, but its Act does not generally apply to media/press organisations or professional journalists, for the purposes of journalism. These 'media users' have an obligations to hold the data securely, and to provide some facility to consider complaints, but these provisions will not place legal restrictions on the uses they can make of personal data. So while journalists may have complete exemptions in Japan, this is unlikely to apply to a company like the developer of the DNE app.

The **Philippines** is somewhat similar to Japan. There is no express exemption for any form of publicly available information, but personal information processed for 'journalistic, literary, artistic or research purposes' is exempt from the Act. Use and disclosure of personal data is prohibited unless the data subject has given express or implied consent. However, there is an ill-defined and potentially very broad exception where the processing is necessary for the legitimate interests of the controller or third parties to whom the data is disclosed, except where those interests are over-ridden by the constitutional rights of the data subject. It is impossible to predict whether non-journalistic commercial uses of personal data such as the DNE app would qualify as 'necessary for the legitimate interests' of its developer, and whether they would override the data subject's constitutional rights relevant to privacy.

Taiwan's law is similarly ambiguous. It does not have any specific exemption for publicly available information, but does have an exception for uses outside the purpose of collection 'to promote public interests', coupled with another exception for collection and processing 'related to public interest'. Another exemption 'where it is necessary to prevent harm on the rights or interests of other people' is also extremely broad. These provisions seem to support a broad 'media exemption', but could be interpreted to go further and allow non-journalistic commercial publications of publicly available information.

At the less-privacy-protective end of the spectrum are the jurisdictions that, in various ways, place few restrictions on the use of personal data once it is 'publicly available'. **Singapore**'s Act is perhaps the most clear, exempting completely 'personal data that is generally available to the public', so that it is the data itself that is exempt, no matter what is done with it. **India**'s 'Rules' under s43A of its IT Act only limit the uses of 'sensitive' personal data, and explicitly exempt 'any information that is freely available or accessible in public domain' from the definition of 'sensitive' data, so there are no restrictions on re-use of publicly available data there.

---

[5] Christopher Kuner *European Data Protection Law: Corporate Compliance and Regulation* (2nd Ed, OUP, 2007), p. 93. Kuner provides references to the specific provisions in the Directive, selected European laws, and court decisions.

Malaysia limits the definition of personal data to 'information in respect of commercial transactions' and also limits the scope of the Act to 'personal data in respect of commercial transactions', and with no application to government agencies. So, information is outside the scope of the Act while it is held in a government-operated public register, and permanently outside the Act if it has nothing to do with commercial transactions. But what if it is information 'in respect of commercial transactions' that is subsequently re-used in a commercial context (like the DNE app)? It is unclear from the Act what happens once the private sector starts using the data in 'commercial transactions'.

Conclusion – Businesses should 'handle with care'

The relatively simple lesson from the Do No Evil decision is that, in Hong Kong and jurisdictions like it, data users cannot regard information extracted from public registers as simply being in 'the public domain' and able to be used for any purpose. When personal data is involved, a more complex set of considerations come into play in order to protect data subjects against uncontrolled use of their personal data in ways that may harm them. In the Hong Kong case, these restrictions and complexities were sufficient to cause the closure of an apparently successful business established in disregard of them. Other situations will require different considerations and may raise fewer problems. Re-use of information which is public because it is published in newspapers or books is likely to raise fewer problems, but each type of Internet publication would need separate consideration. Journalistic uses (including of public register information) have broad exemptions from data privacy laws in most jurisdictions.

In Hong Kong, Macau, South Korea, Japan, the Philippines and Taiwan a high level caution is needed. Only in Singapore and India do there seem to be no problems likely in use of publicly available personal data, and that may well also be the case in Malaysia. Overall, the only safe approach to re-use of publicly available personal data in Asia as a whole is 'handle with care'.