Japan: Toward international standards – except for 'big data'

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

9 June 2015; *Privacy Laws & Business International Report*, Issue 135 (June 2015)

In June 2014, the Japanese government released details of its proposals[1] for the first significant changes to its data privacy law of 2003, the *Personal Information Protection Act* (PIPA). The proposals, which were quite unclear, appeared to do little to improve the weaknesses of the Japanese law compared with international standards (or most other laws in Asia or elsewhere), and were explicitly presented as intended to make it easier for 'big data' processing of personal information.[2] A further iteration of the proposals maintained this impression,[3] including that the proposed data protection authority would be without significant powers.

A year later, the Bill[4] introduced into Japan's Diet in March 2015, and now nearing enactment, presents a significantly different picture: reforms which will bring Japan's closer to international standards for privacy principles; and a new data protection authority which has significant powers, and requirements to act independently. While the 'big data' provision concerning use of 'anonymised' data are still included, there are significant controls on business use of such data. That Bill has been passed unchanged by the lower House of Japan's Diet in May 2015, and is expected to be enacted unchanged by the upper House during June, despite business interests pushing for a number of changes. This article analyses the Bill's proposals, and reaches some conclusions about what will be needed to make them effective.

The PIPC: A data protection authority at last

The current Japanese law is 'Ministry-based', with each Ministry supposed to enforce the Act in its industry sector, and no central authority responsible for data

[1] Government of Japan, Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) 'Outline of the System Reform Concerning the Utilization of Personal Data' (24 June, 2014) <http://kipis.sfc.keio.ac.jp/wp-content/uploads/2014/07/English-Translation-of-Japanese-Government-Proposal-on-Privacy.pdf >

[2] See Graham Greenleaf 'Japan's proposed changes: Weaken privacy to foster 'big data' ' (2014) 130 *Privacy Laws & Business International Report*, 23-25 <http://ssrn.com/abstract=2517193> .

[3] Cabinet Secretariat, IT Strategy Headquarters, Personal Data Commission 'Outline of Legislative Bill on the Institutional Revision for Utilization of Personal Data (Draft)' December 19, 2014.

[4] This article is based on unofficial English translation of the Bill, and of the 2003 Act, as amended by the proposed Bill. Quotations have been checked by Japanese experts, but all interpretation is by the author. Assistance has also been provided by a presentation by Professor Hiroshi Miyashita at the 'Asia-Pacific Roundtable: Understanding Asia-Pacific data privacy laws' (Privacy Laws & Business) on 27 May 2015.

protection. Since 2007 there has been debate within Japanese official circles[5] about establishment of a data protection authority (DPA), as is found in 90% of countries with data privacy laws. From 2014, a 'mini-DPA', the Specific Personal Information Protection Commission (SPIPC) was established solely to regulate Japan's new ID number system. The Bill will incorporate this 'specific' DPA into a new 'general' DPA, the Personal Information Protection Commission (PIPC), which will have jurisdiction in relation to the whole private sector, but not the public sector. Supervision of the public sector will be by the Ministry of Internal Affairs and Communications (MIC), except that the PIPC can ask for reports to be made to MIC.

The PIPC has strong provisions concerning its independence (Arts 59-74). It will consist of a chairperson and eight commissioners, appointed by the Prime Minister with the consent of both houses of the Diet. It must include experts on protection and proper and effective use of personal information, consumer protection, IT, administration relevant to the ID number, and business (Art 54(4). Tenure of members is for five years, subject to reappointment, and is protected against dismissal except for defined forms of misconduct. The chairperson, appointed by the government, will manage the Commission's affairs. It can request the appointment of short-term expert members to investigate technical matters. The PIPC will be under the jurisdiction of the Prime Minister, but the chairman and members are explicitly required to exercise their authority independently (Art 62). Perhaps the most important task of the PIPC will be to formulate the PIPC Rules to implement the Act or Cabinet Orders (or based on special delegation in laws or Cabinet Orders). Much of the delegated legislation concerning data privacy will therefore be made under the independent authority of the PIPC.

Veteran Japanese privacy expert Professor Masao Horibe is the Chair of the existing SPIPC, and as such he will become the first Chair of the PIPC,[6] from 1st January 2016.

The PIPC's enforcement powers

The PIPC has significant powers, if it chooses to use them, and is given sufficient resources to do so effectively. It has explicit functions to receive complaints and mediate in them (Art 61), and powers to investigate ('request reports') and give advice (Arts 40, 41), find breaches, make recommendations, and if they are not followed, give orders that they must be followed (Art 42). Matters relating to the ID system must be investigated under separate procedures. Unlike some DPAs with stronger powers, the PIPC cannot issue its own fines or 'administrative penalties', this depends on prosecution (Arts 84, 85).

These are all normal provisions for data privacy legislation, but much stronger than in previous drafts of the government's proposal. Ministries no longer have these powers via this Act, or probably under any other Act. Ministries may refer apparent

[5] For details, see Graham Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), pgs 235-7.

[6] Article 7 of the supplementary provisions provides interim measures that the SPIPC Chair and its members will be the Chair and the member of the PIPC.

breaches of the Act by businesses normally under their jurisdiction to the PIPC (Art 45). The PIPC may also, in cases of urgency, or due to other circumstances specified in a Cabinet Order, delegate its authority to request reports to a Ministry, but the Ministry must then report the result to the PIPC (Art 44). Unless this last provision is used excessively, it seems that the PIPC will not have its central role removed from it – but that is a danger that needs to be watched. The PIPC therefore seems to have been placed in the centre of Act, not the periphery.

Unfortunately, fines for breaches of the Act's provisions will still have a trivially small maximum of ¥300,000 (US$2,500).[7] It seems as though a few zeros have been omitted, compared with the levels of fines now occurring in the USA or the EU.

There has been very little serious enforcement of Japan's data privacy law in the past decade.[8] The powers given to the PIPC provide an opportunity for a fresh start, but the fines that can follow breaches do not reflect a new level of seriousness.

The PIPC will also take over the authorization and supervision of the authorized personal information protection organisations (APIPOs), sectoral industry bodies that are supposed to mediate in relation to complaints concerning businesses in their sector, and to issue guidelines to businesses in the sector (Arts 47-57). This form of co-regulation in Japan has been criticized by official investigations and has not been successful,[9] but may become more effective under PIPC supervision.

Consumer benefits from stronger principles

Japan's current law has the weakest privacy principles of any Asia-Pacific country that has a data privacy law.[10] The Bill includes changes to address such criticisms, including the following:

- *Restrictions concerning overseas transfers of personal data* have been added for the first time (Art 24), although they are very weak restrictions. Unless an exception operates, the business must obtain the consent of the data subject to their personal data being provided to a third party located overseas (but without any further details being necessary). There are three exceptions allowing exports: (i) to a country included in the PIPC Rules in a 'White List' of countries acknowledged as providing the same level of privacy protection as Japan; (ii) in situations listed in Art 23(1), based on statute or the protection of others; or (iii) to overseas businesses that have established a system complying with the PIPC Rules for a business to 'continuously take

[7] There is also a higher penalty of ¥500,000 for offences concerning misappropriation of databases for an illegal purpose (Art 83)

[8] Graham Greenleaf and Fumio Shimpo 'The puzzle of Japanese data privacy enforcement' *International Data Privacy Law* (2014) 4 (2): 139-154; for a different perspective see Hiroshi Miyashita 'Personal information protection and its enforcement mechanism in Japan' (2014) 8(2) *Sungkyunkwan Journal of Science and Technology Law* 103-115.

[9] Graham Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014), p 260.

[10] Greenleaf *Asian Data Privacy Laws,* Chapter 17.

measures' to provide protection. This last exception, which has very general wording, may be designed to allow overseas businesses certified under the APEC Cross-border Privacy Rules system (CBPRs) to comply.

- *Requirements to allow a person access (called 'disclosure') and correction* of personal data capable of identifying them are now more explicit. Article 28 requires the business to disclose the information requested without delay, subject to specified exceptions, and to investigate a request for exceptions, act upon the result of the investigation by making corrections etc, and advise the person of the result.

- *A requirement of deletion* is now provided: A business operator must erase personal data promptly when it is no longer necessary for the purposes of the business (Art 19). Provisions requiring discontinuation of use of data in breach of the Act, upon request, are also more clearly expressed (Art 30).

- *Sensitive personal information* (as it is often called elsewhere) is given additional protection for the first time, as personal information requiring special consideration (or protection). The categories of information to be given special consideration must be first specified by Cabinet Order, although some possible types of information are listed,[11] and the objective is stated to be that persons will not be subject to unfair discrimination or prejudice. Such 'special consideration' information (once specified) obtains only two types of extra protection: it cannot be collected without prior consent, unless exceptions apply (Art 17(2)); and it cannot be disclosed to third parties after the mere giving of notice via a website (Art 23(2)).

- *The exception for disclosure of personal information* to third parties, simply by a business giving notice of such disclosure via a website, with an option to the data-subject to opt out, is one of the weakest aspects of the current Act. Businesses must now notify the PIPC when they do this, and the PIPC must 'publicly announce' that it has occurred. That is a minor improvement for consumers, but the important thing is that the government's previous proposal to introduce a similar 'notice and opt-out' approach to changes to internal uses of personal data has been dropped (Art 23 (2)-(4)), after opposition from consumer advocates in Japan.

- *Cooperation with overseas privacy enforcement agencies* is now explicitly allowed (Art 78).

These changes, once enacted, will bring the principles in Japan's law to a similar position to most other Asian or Asia-Pacific countries with data privacy laws:

[11] The special categories may include (but are not necessarily limited to) those '… such the person's race, religion, social status, medical history, criminal record, and history as a crime victim' (Art 2(3)).

stronger than the basic OECD principles, and about mid-way toward the 'European' principles of the EU Directive or the Council of Europe Convention.[12]

'Anonymous processed information': Trying to define 'big data' processing

The new concept of 'anonymous process information' (API) is defined as 'information related to an individual that was obtained by processing personal information such that a specific individual cannot be identified, and so that such personal information cannot be restored…' (Art 2(9)). This objective must be achieved by taking the measures detailed in the rest of Art 2(9), which correspond to two categories of 'personal information' in Art 2(1).

For one category, where the information contains 'an individual identification code' (defined in Art 2(2) and including biometrics), it must be achieved by 'deleting all of the individual identification codes contained in the personal information (including replacing such individual identification codes with other individual identification codes in a random manner that will not allow the restoration of the individual identification codes).' In the other category (where it does not contain 'an individual identification code'), anonymisation is supposedly achieved by 'deleting a part of the descriptions and the like contained in the personal information (including replacing such descriptions with other descriptions in a random manner that will not allow the restoration of the part of the descriptions).'

These procedures have been set out in full because it is questionable whether experts on de-identification would agree that such steps would necessarily succeed in achieving anonymisation in the required senses 'that a specific individual cannot be identified, and so that such personal information cannot be restored'. The PIPC Rules must also to set out standards which business operators must follow to achieve those goals (Art 36(1)). This provision may therefore allow PIPC to prescribe procedures to achieve an objective that they cannot realistically always achieve. If so, this will make how the provision will be interpreted impossible to predict, creating uncertainty for businesses and consumers.

Putting that potential problem aside,'business operator handling [API]' is defined as a private sector body that uses information including API that is configured systematically to enable searching (Art 2(10)). Such business operators have significant obligations (Arts 36, 37). If they create API, they must take security precautions, so as to prevent either deleted information or their method of anonymisation being divulged. They must publicly announce the items of information relating to individuals contained in the API, and whether and how they are going to disclose it to third parties. They must tell third parties that they are receiving API. Anyone using API (whether or not they created it) is forbidden from comparing it with other information in order to attempt to re-identify it. Anyone handling API must take security measures concerning it, must have a complaints procedure concerning it, and must endeavour to make such measures public. They

[12] Greenleaf *Asian Data Privacy Laws,* pgs 502-5.

must take the same steps in relation to any other recipients of the API. They must do all of this according to provisions in the PIPC Rules.

Therefore, although API is not 'personal information', many protective provisions similar to those applied to personal information apply to API. Business organisations in Japan, and any outside Japan who might need to comply with Japanese law on these matters, will need to consider carefully the business case for the creation and/or use of API, given the significant obligations, and uncertainties, that accompany it.

Conclusions: Will too much depend on the PIPC?

Many of the key details on which the operation of the revised Act depends will only be found in the PIPC's 'Rules'. This is obvious in relation to API, but also applies to many other aspect of the Act, and on the implementation of Cabinet Orders. The PIPC will make exceptions allowing collection of 'special consideration' information; draw up a 'White List of countries'; control how businesses can expand disclosure through opt-outs; make standards for every aspect of 'anonymous process information'; supervise and issue guidelines for APIPOs; and much more.

The real effectiveness of the new Act is therefore going to depend a great deal on the chairperson and members of the PIPC (when appointed), on their exercise of their independence, on their willingness to enforce an Act that has not previously been enforced, and on the resources provided to them to do so.

Despite this Bill bringing Japan's data privacy law closer to international standards, other factors will reduce its consistency with laws of other countries. The law will be administered very differently in the public and private sectors. The distinction between personal information and anonymous processed information (API) will be a unique feature of the Japanese law. It remains to be seen how it will operate, and whether it will have any international influence.

Professor Fumio Shimpo of Keio University, Japan and Professor Hiroshi Miyashita of Chuo University, Japan, have provided helpful information for and comments on this article, but all content remains the responsibility of the author. Privacy Laws & Business International Report will publish a further article by Professor Miyashita on the new Japanese law once it is enacted.