Japan's proposed changes: Weaken privacy to foster 'big data'

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

(2014) 130 *Privacy Laws & Business International Report*, 23-25

Japan is proposed the first significant changes to its data privacy law of 2003, the *Personal Information Protection Act* (PIPA). The proposals are set out in an 'Outline of the System Reform' published by the government's 'IT Strategic Headquarters' in June 2014.[1] Submissions were called for within four weeks. Now, according to the government, 'the Cabinet Secretariat will play a central role in the adjustment of issues among all government ministries and amend the direction as needed' with the aim of introducing a Bill as soon as possible after the session of the Diet commencing in January 2015. All quotations in this article are from the 'Outline'.

Those attempting to understand what the Japanese government is planning have to contend with the 'Outline' being very confusing: it has ten main sections, and any one issue and related proposals will very often be dealt with in multiple sections, in different terms. The more concrete proposals are in the final sections. There is also very clearly dissension within the members of the 'IT Strategic Headquarters.' Experts involved in the process confirm that very little in the proposals is yet settled, and that the Japanese language version of the 'Outline' has no greater clarity than the English translation.

This article explains and critiques the Japanese government proposals from a consumer and data subject perspective.

New 'reduced identifiability' aims to capitalise on 'Big Data'

The underlying purpose of the reforms is primarily to facilitate businesses and government being able 'to utilize personal data including the behaviors and states of individuals, which has a high usage value, not only for the benefit of individuals, but also for the public interests.' This is so that Japan can take advantage of 'Big Data' analysis techniques 'to significantly contribute to the ongoing creation of innovation in Japan through the emergence of new industries and services'. It is perceived that a 'Gray Zone' exists, 'where it is unclear as to whether the free use of information is allowed has emerged and expanded', with the result that 'the extent to how far personal data should be protected and the rules that govern business operators are becoming more ambiguous.' The core of the proposed reforms is therefore the creation of a category of 'reduced identifiability' information about individuals, to which at least some normal rules concerning personal information will not apply, particularly requirements of consent in relation to use and disclosure.

While 'breaking down the "Barriers to Utilization" of personal data of high usage value is critical', in the government's view, and clearly the driving force of the reforms, clearer definitions of personal data are 'needed to assure consumers their information is securely protected'. The strongest policy statement from a consumer perspective is that '[t]o ensure

[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 Utilizationof 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>

business operators' compliance with the rules, and obtain the consumers' trust, it is necessary to enforce the system appropriately by the fair and independent enforcing body.'

From a consumer perspective, the proposal to remove most privacy protections from supposed 'reduced identifiability' data will depart from current international standards for 'personal data' and put Japan out-of-step with other countries, rather than in advance of them. No standards for de-identification are proposed,[2] and it seems that it will be essentially a self-regulatory system, with some role for guidelines to be 'accredited' by the proposed DPA ('3rd party organization).[3] No penalties are proposed against any party if data is in fact re-identified, but the possibility of penalties is reported to be under discussion. This could become little more than a 'best efforts' requirement, with no consequences for 'failure' to de-identify. If so, it could destroy protections for consumers, reducing consumer confidence in e-commerce, and pose a moral hazard to businesses.

Some weaker and few stronger principles proposed

.Japan's *Personal Information Protection Act* (PIPA) has the weakest privacy principles of any Asia-Pacific country that has a data privacy law.[4] As well as the lower standard of 'reduced identifiability, the rest of the government's proposals will, overall, weaken the principles in Japan's law, although they do have some positive aspects.

Change of use – Japan already has low standards for both change of use (allowing 'duly related' uses) and disclosure to third parties (an 'opt out' procedure – see PIPA art. 23). It now proposes to have an 'opt out' for any change of use, without need to directly notify individuals (a notification to the DPA and publication may suffice). This is not found in any other country's law, will reduce consumer protection, and may not comply with the OECD Guidelines.

Deletion – No requirement of deletion of personal data at any time is in the current PIPA, and none is now proposed. Business might be required to publish deletion / retention periods. Almost all countries now require deletion when use is completed, including 7/11 Asian jurisdictions with data privacy laws.

Access, correction and stopping use – It is not clear under PIPA how a consumer is able to insist on their rights of access or correction, a very rare deficiency in data privacy laws. The proposals state that 'Regulations shall be put in place related to the person's right to disclosure, correction, discontinuation of utilization etc'. Disclosure seems to mean 'access'. The right to access will be limited (as now) in 'burdensome' and 'frivolous' cases. It is implied that the DPA will have a role in enforcing these rights, but 'judicial exercise of the right' is also mentioned. It is desirable that the right of access, and all other individual rights, should be enforceable by the new DPA ('3rd party organization), and also by judicial bodies.

---

[2] It is unclear what is meant in the 'Outline' by 'Necessary measures shall be taken to define the procedures to be followed by the business operators handling personal information in the cases where individuals can be identified without the persons' knowledge, as a result of information being collected, matched and analyzed.' There is also a reference to 'countermeasures against possible abuse resulting from data analysis'.

[3] The proposals refer to 'multi-stakeholder' processes (MSPs) which will include businesses, government, experts and consumers. It is not clear which rules these MSPs will make. Such processes usually disadvantage consumers. They are unbalanced because business and government can always afford to better represented, more often, and for meetings in increasingly remote locations as the decisions to be made become more important. At worst, this will allow business to write its own rules. Such processes are not used to develop data privacy laws anywhere, including in the USA where they are moribund.

[4] G Greenleaf *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, forthcoming October 2014), Chapter 17.

Sensitive information – PIPA does not at present include any definition of, or special rules about, 'sensitive information'. The 'Outline' says 'data that may cause social discrimination, such as race, faith, social class and criminal records etc' will be defined as 'sensitive information'. The basis of use of such data will be consent, with some exceptions allowed. It does not say that sensitive information will be excluded from what can become 'reduced identifiability' data (for which no consent to use will be required), but perhaps that is why such a definition is now considered necessary. The proposals to define categories of 'sensitive information' and give them additional protections are desirable, provided that protections for other personal data are not weakened.

'Small business' exemption – The current exemption from PIPA of businesses handling personal information on fewer than 5,000 individuals is proposed to be abolished, but replaced with a vaguely stated exemption for business 'considered unlikely to violate the individual's rights and interests unless such business operator has a history of committing a breach of obligations intentionally or by gross negligence'. This is likely to be at least as bad, from a consumer perspective. How will a consumer ever know they are dealing with an exempt business? How will a business accumulate an adverse history if it is already exempt from any obligations? If used as a broad exemption, this could equate to a partial repeal of PIPA.

Enforcement – Internecine disputes, unclear intentions

It is clear is that stronger protection of privacy plays a lesser role in the policies behind these reforms, but at least on the enforcement side it is not being ignored.

Enforcement of PIPA is at present minimal.[5] No Ministerial orders or prosecutions occur. Industry complaints bodies do very little. There is no clear procedures for individual complaints to be made. There is little transparency, and in particular no published results of complaints. Individuals cannot enforce PIPA in court to obtain compensation for breaches, following a Tokyo High Court decision. As a result, individuals have no effective enforceable rights under Japan's law. The cumulative effect is that PIPA does not meet international standards for enforcement. Strong reforms, including a central Data Protection Authority (DPA), enforceability and transparency are needed if Japan wants global credibility for its law.

The following comments reflect a consumer-oriented critique of the government's proposals in relation to enforcement, as far as they can be interpreted at present.

A data protection authority? – The proposal to create what is called a '3rd Party Organisation', but would elsewhere be called a data protection authority ('DPA' hereinafter), is desirable if it has strong enough powers and responsibilities. No composition of the proposed DPA is proposed, other than that it would be independent of Ministries. A strong DPA is necessary to give central coordination, direction and consistency, and a central locus for individual complaints and remedies. Japan's current decentralized dispersal of authority between Ministries, local government bodies, and many semi-official industry and consumer bodies, is not effective.

Limited DPA functions – To enforce PIPA in the private sector, the 'Outline' says the proposed DPA 'shall have the function and authority to conduct on-site inspections in addition to the function and authority the relevant Minister currently has for business operators handling personal information.' Unfortunately, these existing powers are very

[5] G Greenleaf and F Shimpo 'The puzzle of Japanese data privacy enforcement' *International Data Privacy Law (2014) 4 (2): 139-154 < http://idpl.oxfordjournals.org/content/4/2/139.abstract>.*

limited, with Ministers currently not having any powers to fine businesses for breaches, or award compensation, or even any clearly stated powers to investigate individual complaints. The DPA is to 'certify' rules that are developed by self-regulatory 'multi-stakeholder processes'. It is to 'certify business operators wising to engage in cross-border data transfer'. Otherwise, its proposed functions are very limited: to collect and publish opt-out notices; liaise with overseas DPAs (including via APEC CBPRs, it may be assumed); advise the Prime Minister and report to the Diet; collect reports from Ministries; and carry out PR.

No clear dispute resolution or enforcement powers – What is missing is that the proposed DPA has no clear role in complaint resolution, nor is it clear that it will have powers to order fines or compensation. The 'Outline' only says that a 'dispute resolution system … shall continue to be studied'. The need for penalties to 'ensure the effective exercise' of the DPA's powers is stated, but also that discussion of the 'needs and purposes' of an 'administrative monetary penalty system' is continuing. Most existing DPAs, or alternatively courts, have such powers, including in Asia. Almost ninety countries have DPAs. Japan's DPA needs to at least have powers to issue administrative fines, and to investigate and order remedies in relation to individual complaints (or refer such cases to an independent tribunal or court for final decision). These are the minimum standards met by other DPAs in the world. In short, it is not clear that this proposed DPA is intended to enforce Japan's law in any serious sense – and no other body does so at present.

Ministries to retain powers? – It is clear from the government's proposals that at least some Ministries are trying to retain as much of their sectoral powers as possible, and are attempting to ensure that any '3rd party' DPA does not have any serious powers within their sectors: 'involvement of each Minister shall be considered based on the arrangement of the relationship between the Minister and Third Party Organization'. These attempts need to be resisted by the government, because the feudal Ministry-centred nature of Japan's privacy law has made it ineffective. Business and consumers need consistent central guidance.

No public sector coverage? – Government Ministries and agencies are also resisting having a DPA with enforcement powers over complaints against public sector agencies. Japanese citizens need an effective avenue to pursue public sector privacy complaints, which they do not have at present. If Japan does create a DPA, but it has no jurisdiction over Japan's public sector privacy laws (except perhaps the ID number), it will be the only DPA in the world in such an invidious situation. This will not assist the international reputation of Japan's law. The government should insist that the DPA covers the whole public sector in all its activities.

Individual rights – Individuals have at present no right to sue in court for damages for breaches of PIPA. Most data privacy laws give a right to damages from either a court or DPA, including all European laws, and all data privacy laws in Asian countries except Malaysia and Japan. The proposals should include a right to obtain damages (including for non-pecuniary harm) from either the DPA or a court (or preferably either).

Transparency? – The proposals do not include any requirements of transparency of enforcement by publication of the outcomes of individual complaints. Other DPAs in Asia (eg Hong Kong, Korea, Macau) publish such case summaries, as do many in other jurisdictions including the USA's Federal Trade Commission. Publication of such summaries, as well as statistics, should be required.

Data exports and imports

Japan does not currently impose extra restrictions on personal data exports. What the 'Outline' is proposing is very unclear, but states that exporters 'must undertake measures such as concluding agreements that require [the recipients] to undertake necessary and

appropriate measures to ensure the secure management of personal data', but without further details of the standard to be required. The private sector bodies authorized by the DPA will also have some role to 'review compliance with the privacy protection standard accepted by counterparty country and then certify business operators wishing to engage in cross border data transfer', but again the standard of such certification is unstated. At another point, the 'Outline' states that the DPA will itself 'review compliance with the privacy protection standard accepted by the counterpart country and then certify business operators wishing to engage in cross border data transfer'. Whichever is correct, it seems that data exports from Japan will have to meet some standard for the first time.[6]

It is also implied that PIPA will have some extra-territorial operation, because 'it is not clear whether [PIPA] applies to business operators that use personal data at facilities outside Japan.' In relation to facilitating data imports into Japan, the 'Outline' seems to imply that Japan's involvement in APEC's CBPR system will involve the new DPA as the 'enforcement agency' for Japan,[7] but also that there will be some involvement of 'each Minister' in enforcement. How important this will be is uncertain, since neither the EU nor anyone else yet accepts the APEC CBPR approach as satisfying their data export requirements.[8]

Conclusions – One hand clapping?

It is clearly desirable that the Japanese government should revise its data privacy law after a decade of moribund operation, including by making it more clear in its operation to assist businesses and consumers, and by providing a DPA as a central point of policy direction and enforcement. However, this need not involve weakening protections for consumers. It should not do so, because both the principles and the enforcement of Japan's law need strengthening and made more transparent to meet consumer and citizen interests. Japan's data privacy law would also be more internationally credible if it was more consistent with standards adopted internationally, rather than by overly aligning it with the positions and interests of US-based global businesses with business models based on invasion of privacy, including those so prominent in e-commerce in Japan. In particular, it is not clear how it will assist Japan, or many Japanese businesses, to adopt a radical departure from the meaning of 'personal information' that has evolved over the past 40 years. Japan can find better ways to improve socially valuable utilization of personal data than this ill-considered approach. Listening too intently to the applause of the American Chamber of Commerce in Japan[9] will involve the risk of listening to one hand clapping.

---

[6] The extent to which the Act has extra-territorial effect to businesses using personal data outside Japan is also to be clarified, but how is not stated.

[7] The "Outline' refers to the DPA authorizing the private sector certification bodies, but that is not how APEC CBPRs works.

[8] G Greenleaf and N Waters 'APEC's CBPRs: Two years on – take-up and credibility issues' (2014) 129 Privacy Laws & Business International Report, pgs. 12-15.

[9] Submission by the American Chamber of Commerce in Japan to the government of Japan< kipis.sfc.keio.ac.jp/commentary-on-2014-japanese-privacy-law-revisions/>