University of New South Wales Law Research Series

Questioning 'adequacy' (Pt I) – Japan

GRAHAM GREENLEAF

(2017) 150(1) *Privacy Laws & Business International Report*, 6
[2018] *UNSWLRS* 1

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Questioning 'adequacy' (Pt I) – Japan

Graham Greenleaf, Professor of Law and Information Systems, UNSW Australia*

(2017) 150 *Privacy Laws & Business International Report*, 1, 6-11

Assessments by the European Commission of whether non-EU countries provide an 'adequate' level of data protection so as to enable a positive EU decision[1] under Article 25 of the 1995 data protection Directive ('adequacy decisions') usually receive little discussion while the process is underway. It is often not until the near-final stage of decision-making, when the Article 29 Working Party (A29WP) of data protection Commissioners gives an Opinion on whether it supports a positive assessment by the Commission, that it even becomes public knowledge that an assessment is taking place. There are exceptions, such as the assessments of the USA's original 'Safe Harbor' scheme,[2] and subsequent 'Privacy Shield' scheme.

Where the Commission reaches a negative opinion after an assessment, as has occurred twice in relation to India, no recommendation goes to the A29WP, no Opinion is issued, and the reasons for a negative assessment (or even the fact that it took place) are usually little-known. Positive determinations of adequacy have only been made for eleven jurisdictions[3] and for certain passenger information arrangements. 'Adequacy' remains opaque, after 20-plus years.

It is therefore unusual that both Japan and South Korea made public in 2016 that they were applying for positive adequacy assessments by the EU, and that general comments about these assessments progressing have been made by the Commission and by representatives of the two countries. Japan and the EU are considering simultaneous findings of adequacy, which Japanese law also allows.[4] Even more unusual is that Korea decided to make its own 'Self Assessment' of the adequacy of its data protection in 2016, and then updated it in 2017 after changing the scope of the assessment sought.[5]

The two parts of this article, after providing brief background on the 'adequacy' process, first consider the position of Japan (which the EU is considering first) and then (in Part II), Korea, in relation to the criteria that the EU uses to assess adequacy. The articles focus on identifying

* The assistance is acknowledged of Prof. Lee Bygrave, both from valuable comments, and from earlier joint work on adequacy assessments, and of Prof. Fumio Shimpo, and Prof. Hiroshi Miyashita, both of whom have been very generous with their time and expertise. All responsibility for content remains with the author. Declarations of interest: in 2016 I carried out a consultancy assignment for a Korean agency, KISA, to assist it to prepare for Korea's application to the EU for an adequacy assessment; in 2012 I received a three month fellowship from a Japanese academic fund to research Japanese and other Asian data privacy laws, in Japan.

[1] Normally, the Commission makes such decisions on the basis of input from the A29WP, the Committee of Member States (CMS), and the European Parliament, but if the CMS does not approve the decisions it may refer the matter to the Council for final determination: see Articles 29-32 of the Directive. The CJEU may also play a role, as became evident in *Schrems*.

[2] However, the Commission never formally assessed the adequacy of the US legal regime, a deficiency which the CJEU identified in *Schrems v Data Protection Commissioner* (6 October 2015) Court of Justice of the European Union (Case C-362/14) ('*Schrems*').

[3] Switzerland, Canada, Argentina, the Bailiwick of Guernsey, the Isle of Man, Jersey, Israel, Andorra, Uruguay and New Zealand. A second determination in relation to the USA ('Privacy Shield') has been made.

[4] 'Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection', 4 July 2017.

[5] I was the lead author, for a committee of Korean experts, of the 2016 'Self Assessment', but was not involved in the 2017 Update.

issues which may be regarded as negative factors by the Commission, which it will have to consider and balance against the positive aspects of each application.

While such discussion is needed, there is no attempt in these articles to suggest what the Commission's conclusions should be, or might be, in the case of either country. Any proper assessment of a country's claims to adequacy of data protection is likely to take hundreds of pages, not a short article. Nevertheless, there needs to be public discussion of the strengths and weaknesses of the data protection offered by candidate countries, prior to any assessment being made, because of the importance of such decisions for both international trade, and for the protection of human rights. There also needs to be critical consideration of the quality of the decisions made by the EU bodies involved, once they are made, and analysis of what can be learned from them in relation to future assessments.[6] These needs are relevant to both adequacy assessments under the existing Directive, and to the equivalent adequacy provisions (arts. 44-46) of the General Data Protection Regulation (GDPR) which will be formally applied from 25 May 2018. 'Adequacy' is here to stay.

Criteria for assessing adequacy under the Directive

The criteria which have been used within the EU for the assessment of adequacy derive partly from the Directive itself, from the *Schrems* decision, and from the opinions of the A29WP. A simplified version of these complex criteria follows. *[Note: This article was written before the Article 29 Working Party's 'Adequacy Referential (Updated)' (November 2017) was available, but it makes no substantive difference to this article.]*

The Directive sets out general criteria for assessing adequacy. All circumstances surrounding data transfer operations are relevant. Account must be taken not only of formal legal rules and legislatively established oversight mechanisms, but must also take into account (for example) professional and industry practice and standards and other non-legal rules, provided they are complied with. Other contextual factors must also be considered such as the strength of the rule of law, the extent to which the country's administrative and corporate cultures are law-abiding, and the country's international commitments.

The 2015 *Schrems* decision,[7] the first CJEU decision interpreting the concept of 'adequacy',[8] establishes additional criteria which must be met be before the Commission makes a positive adequacy assessment: (a) the country must ensure a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the Directive, read in the light of the EU Charter of Fundamental Rights (particularly arts. 7 on privacy and 8 on data protection)[9]; (b) this level of protection must also apply to the country's public authorities (at least in relation to data within scope of the adequacy assessment); and (c) legislation must enable an individual to pursue legal remedies for access to, and correction of, personal data.

---

[6] G Greenleaf and L Bygrave ' Not Entirely Adequate but Far Away: Lessons from how Europe Sees New Zealand Data Protection' (2011) 111 Privacy Laws & Business International Report, 8-9 :< https://ssrn.com/abstract=1964065 >

[7] *Schrems,* concerning the assessment of the US 'Safe Harbor'.

[8] There are CJEU decisions on the meaning of independence of data protection authorities which are relevant to the question of adequacy: *Commission v Federal Republic of Germany*, judgment of 09.03.2010 (Case C-518/07); *Commission v Republic of Austria*, judgment of 16:12:2012 (Case C-614/10); and *Commission v Hungary*, judgment of 08:04:2014 (Case C-288/12); and see Greenleaf G 'Independence and structure of data protection authorities: International standards and Asia-Pacific experience' *Computer Law & Security Review*, Vol 28, Nos 1 and 2, 2012, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1971627>

[9] EU *Charter of Fundamental Rights of the European Union*[2000] OJ C364/01 and [2010] OJ C83/389.

The Directive does not state which of its substantive principles are essential, or even particularly important, to an adequacy assessment. The Commission's past practice, in obtaining 'expert reports' on candidate countries, has been to adopt the criteria set out by the A29WP's Opinions in 1998,[10] and in 1997,[11] even though these are not legally binding on the Commission. Although these criteria must now be applied in light of *Schrems*, they can be interpreted as consistent with that decision in that they assist in determining when the protections provided by a country are 'essentially equivalent' to those provided within the EU even though they are not identical. The A29WP's headings of the core criteria for adequacy are:

(i) *Content principles:* purpose limitation; data quality and proportionality; transparency; security; rights of access, rectification and opposition; and restrictions on onward transfers.

(ii) *Additional principles* may be applicable to specific types of processing, such as those concerning: sensitive data; direct marketing; and automated decisions.

(iii) *Procedural/enforcement/remedial mechanisms* must achieve provision of: 'a good level of compliance'; 'support and help to individual data subjects'; and 'appropriate redress to the injured parties'.

These criteria were applied in many expert reports to the Commission, including that for the most recent 'whole country' (ie non-sectoral) positive finding, that concerning New Zealand, and a report concerning India, both in 2013. It is also now necessary not to ignore the GDPR, because any new adequacy assessments made under the Directive, although they will remain in force after May 2018 (GDPR art. 45(9)), must be reviewed within at most four years (art. 44(3)), on the basis of new GDPR procedures for assessment which will inevitably involve somewhat different 'core criteria' than those listed above. Also, the GDPR is more specific than the Directive concerning the factors that must be taken into account in adequacy assessments (arts. 44 and 45(2)).

Assessment of adequacy is therefore a complex matter, a question of balancing positives and negatives, and without black-and-white criteria for inclusion or exclusion.

Japan – Issues for adequacy assessment

On 4 July 2017 the European Commission and Japan issued a joint statement[12] which referred to the possibility of a 'simultaneous finding of an adequate level of protection by both sides' (Japan's revised law allows the possibility of such 'white-list' findings), and the objective of 'achieving this goal by early 2018, including by addressing relevant differences'. Japan is expected to only seek an adequacy assessment for its private sector because its Personal

[10] "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" WP 12, DG XV D/5025/98, adopted on 24 July 1998, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf>.

[11] "First orientation on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy" WP 4, XV D/5020/97-EN final, adopted on 26 June 1997, available at <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf>.

[12] European Commission 'Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection Commission of Japan on the state of play of the dialogue on data protection', 4 July 2017 <http://europa.eu/rapid/press-release_STATEMENT-17-1880_en.htm>

Information Protection Commission (PIPC) created under the 2015 revisions to its Protection of Personal Information Act (PPIA) does not have powers over the public sector.[13]

The following comments focus on only a few major issues which may be important to an adequacy assessment: the scope of 'personal information; data export restrictions; and demonstrated enforcement. Many other issues may be relevant to an adequacy assessment of Japan, including the limited scope of sensitive information given additional protections, the restriction of scope to a 'personal information database etc', the extent of many of the 'content principles' and individual rights, and government access to private sector data.

Exempting data 'not readily collated' or 'anonymously processed'

Japan's legislation defines 'personal information' in terms of its capacity to identify an individual[14] (as does the EU Directive and most data privacy laws), but there are two 'carve-outs' from the scope of that definition which may be significant to an EU assessment of adequacy.

The first carve-out is that the most authoritative translation[15] of the definition of 'personal information' says that it includes information 'containing' specified items 'whereby a specific individual can be identified (including those which can be *readily collated* with other information and thereby identify a specific individual)' (emphasis added). This remains unchanged from the original 2003 Act (though some translations referred to '*easy* reference'). If information in two documents cannot be 'readily' (or 'easily') collated/cross-referenced, the information is not personal information, and is outside the scope of the PPIA or any privacy controls. This seems to be a narrower definition than the EU definition of 'personal data', which refers to identifiability 'directly or indirectly' without requiring it to be 'readily collated' or 'easy' to cross-reference.[16]

The second carve-out is that Japan's 2015 amendments to the *Protection of Personal Information Act* (PPIA) introduced a new concept of 'anonymously processed information' (API) which is defined in art. 2(9) as 'information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking action prescribed in each [of arts. 2(9)(i) and 2(9)(ii)] in accordance with the divisions of personal information set forth in each said item nor to be able to restore the personal information'. Such 'anonymity' must therefore be achieved by one of two categories of measures prescribed by PPIA arts. 2(9)(i) and (ii). These provisions require 'deletion' (which includes replacement) of 'descriptions' that contain personal information (art. 2(9)(i)) or 'codes' (2(9)(ii)), corresponding to the two parts of the definition of 'personal information' (art. (2)(1)). Such 'anonymous' information is not regarded by PPIA as 'personal information',

---

[13] Act on the Protection of Personal Information (Japan) (PPIA): effect of art. 2(5) definition 'business operator handling personal information', which excludes public sector bodies. There is no official statement of the scope of the application.

[14] Act on the Protection of Personal Information (Japan) (PPIA), art. 2(4).

[15] Act on the Protection of Personal Information (Translation date : December 21, 2016), on *Japanese Law Translation* website (operated by Nagoya University with government funding) <http://www.japaneselawtranslation.go.jp>. All quotations from the PPIA in this article are from this translation. An earlier translation (February 2016) which was on the Personal Information Protection Commission (PIPC) website was inadequate in relation to this definition because references to 'readily' or 'easily' were omitted. Care must therefore be taken to use the correct (December 2016) translation.

[16] The 1995 EU data protection Directive, Art. 2(a) states " 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity;"

however a few protective provisions similar to those applied to personal information apply to API.[17]

Recital 26 of the Directive says that 'the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'. The EU standards concerning de-identification are best set out in the A29WP interpretation of Recital 26:[18]

> *…data must be processed in such a way that it can no longer be used to identify a natural person by using "all the means likely reasonable to be used" by either the controller or a third party. An important factor is that the processing must be irreversible. The Directive does not clarify how such a de-identification process should or could be performed. The focus is on the outcome: that data be such as not to allow the data subject to the identified via "all" "likely" and "reasonable" means.*

Also, while anonymisation is an instance of further processing of personal data, the A29WP said 'it can be considered to be compatible with the original purposes of the processing but only on condition the anonymisation process is such as to reliably produce anonymised information'.

Comparison of the Japanese provisions with the EU requirements raises a number of issues. First, the Japanese law prescribes methods of producing 'anonymous' information, whereas the EU Directive's approach does not, but instead focuses on the goal of irreversibility, and denies exemption from legislative requirements unless the goal is achieved. More precisely, the Japanese law's approach is that API is defined in art. 2(9) as information 'that can be produced … by taking action prescribed' in arts. 2(9)(i) and 2(9)(ii). Further to this, a business shall, when producing API, 'process personal information in accordance with standards prescribed by rules of the [PIPC]' (art. 36(1)). Article 19 of the PIPC Rules[19] prescribe such standards in five brief non-technical paragraphs describing different methods of 'deletion'. The PIPC has also issued a report on how such API processes would work.[20]

It seems therefore, that if a Japanese business follows the prescribed actions, standards and rules to produce API, the information it produces will be considered as API, not 'personal information', and thus be subject to a lower level of protection, irrespective of whether experts would agree that anonymisation has in fact been achieved. It is questionable whether experts on anonymization would agree that the steps prescribed in arts. 2(9) and 36 of PPIA and art. 19 of the PIPC Rules would necessarily succeed in achieving the goal of preventing re-identification, but that is beyond the scope of this article.

Broadly put, the issue for an adequacy assessment raised by both the definition of 'personal information' and the API provisions, both of which also have parallels in Korea, is whether, in comparison with the requirements of the Directive, they result in exempting from data

---

[17] These protections are summarised in G. Greenleaf, Japan: Toward International Standards – Except for 'Big Data' (2015) 135 Privacy Laws & Business International Report, 12-14, section "'Anonymous processed information': Trying to define 'big data' processing".

[18] Article 29 Data Protection Working Party *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216, 10 April 2014

[19] *Enforcement Rules for the Act on the Protection of Personal Information (Tentative translation)* (Rules of the Personal Information Protection Commission No. 3 of October 5, 2016) (from *Japanese Law Translation* website)

[20] PIPC Secretariat (Japan) 'Toward balanced promotion of personal data utilization and consumer trust' (Report: Anonymously Processed Information), February 2017.

privacy laws too broad a class of what would be personal information in the EU. Both matters essentially enable 'big data' processing, and so they pose for the EU the question of what extent and types of legislated exceptions are compatible with the *Schrems* requirement of a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the Directive and the Charter. It is beyond the scope of this article to suggest an answer to that question, but the assessment of Japanese adequacy brings the matter to the fore because Japan addresses these issues so directly in its legislation – as does Korea in other ways.

Data export restrictions and 'White Lists'

Restrictions concerning overseas transfers of personal data were added for the first time to Japan's law by the 2015 amendments (art. 24). 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 in a foreign country' (but without any further details being necessary). There are three exceptions: (i) a country included in the PIPC Rules in a 'White List' of countries acknowledged as providing equivalent privacy protection to Japan's law; (ii) exceptions listed in art. 23(1), based on statute or the protection of others; or (iii) to overseas businesses that are 'establishing a system' complying with the PIPC Rules for a business to 'continuously take action' to provide equivalent protection.[21]

Concerning (ii), the PIPC has announced on 7 December 2017 draft criteria[22] for a 'White List' of foreign countries under art. 24. As summarised by Prof. Miyashita, a country may be considered if it has a personal information protection system with all the following items;

> *(1) Laws on the business operator of handling personal information;*
>
> *(2) Existence of an independent authority equivalent to the PIPC and its necessary and proper supervision;*
>
> *(3) Cooperation with Japan based on the mutual understanding on the utilization of personal information and protection of rights and interests of an individual;*
>
> *(4) Ensuring data flow mutually with protection of personal information without restricting international data transfer beyond the necessary scope of protecting personal information;*
>
> *(5) Contribution to the new innovation and economic society and realization of life of the citizen in Japan.*

Items (3) and (4) suggest that reciprocity of recognition is expected, as Japan has mentioned in relation to EU adequacy. It is a political as well as a legal assessment.

An APEC CBPRs 'back door'

Exception (iii) seems to be designed to allow compliance by exports to overseas businesses certified under the APEC Cross-border Privacy Rules system (CBPRs). Japan took the final step

---

[21] Technically in the words of the section, 'as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data pursuant to the provisions of this Section'; (Article 24 PPIA).

[22] In Japanese only, at <http://search.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000166934>. Open for public comment until 5 January 2018.

to join the APEC CBPR system in February 2016.[23] Japan's APEC CBPRs membership is not in itself significant to Japan's adequacy application.[24] However, what is significant is that the PIPC Rules (art. 11) state that the 'standards' under PPIA art. 24 'are to be falling under any of each following item', and items (i) and (ii) follow. The advice of Japanese-speaking privacy experts is that the meaning of 'any of each' in the Japanese version is 'any one of' , namely '(i) or (ii)'.[25] So to come within PPIA art. 24, a Japanese business must comply with only one of art.11 (i) or art. 11(ii) in the PIPC Rules, not both of them. PIPC has issued Guidelines[26] concerning Art. 11.

Item (i) is, in summary, where the Japanese exporting and overseas recipient businesses have 'ensured' (by 'Contract, certification, MoU etc'[27]) that the recipient will comply with the key parts of Japan's law, by 'appropriate and reasonable' measures.[28]

Item (ii) refers to when 'a person who receives the provision of personal data has obtained a recognition based on an international framework concerning the handling of personal information', and the PIPC Guidelines confirm that APEC-CBPRs is such an 'international framework' under art. 11 of the Rules.[29]

On this basis, compliance with only (ii) (APEC CBPRs) is necessary, so if a Japanese business proposes to export personal data to a CBPR-compliant business in a country which participates in APEC CBPRs (as yet, only 21 businesses in the US[30]), then it can do so, provided it complies with other aspects of Japan's PPIA. For this purpose, the Japanese exporter's certification under CBPRs is irrelevant, it is the CBPRs certification of the importer that counts. If and when other countries join CBPRs in full, exports will also be authorised to companies that become CBPRs-accredited in such countries. This 'recognition' of CBPRs

---

[23] It appointed the Japan Institute for Promotion of Digital Economy and Community (JIPDEC), as an 'Accountability Agent' (AA)G. For details, see Greenleaf, Japan Joins APEC-CBPRs: Does It Matter? (2016) 144 Privacy Laws & Business International Report, 18-21

[24] This is sometimes misunderstood: see V Gladicheva and M Franklin 'Japan's part in Apec data-transfer system not a big risk for EU privacy deal, official says' *M-Lex Market Insights*, 10 November 2017 < https://mlexmarketinsight.com/insights-center/editors-picks/Data-Protection-Privacy-and-Security/cross-jurisdiction/japans-part-in-apec-data-transfer-system-not-a-big-risk-for-eu-privacy-deal,-official-says>

[25] Concurring advice received from Prof. Fumio Shimpo, and from Prof. Hiroshi Miyashita. Prof Miyashita notes that the PIPC Guidelines do not say anything about the relationship between (i) and (ii). The key question is whether art. 11's reference to 'any of each following item', means that, to come within PPIA art. 24, a Japanese business must comply with both (i) and (ii), or only one of them. In English the most likely interpretation is the latter ('or') but the correct interpretation can only be derived from the Japanese language version. For certainly in an adequacy assessment, it is desirable that a definitive interpretation be obtained, or that PIPC clarify its Rules.

[26] PIPC *Guidelines on the Act on the Protection of Personal Information (Provision to the third party in a foreign country)* November 30, 2016 <http://www.ppc.go.jp/files/pdf/guidelines02.pdf>. The full Guidelines are available only in Japanese. Prof Hiroshi Miyashita has kindly provided an English translation of the Guidelines in relation to art. 11.

[27] PIPC *Guidelines,* concerning Rule art, 11(i). APEC CBPRs compliance is also mentioned under this aspect of the Guidelines, in relation to a Japanese company certified under CBPRs exporting personal data to an overseas agent to process on its behalf, as part of 'appropriate and reasonable' measures.

[28] PIPC Rules, art. 11(i) says 'have ensured in relation to the handling of personal data by the person who receives the provision the implementation of measures in line with the purport of the provisions under Chapter IV, Section 1 of the Act by an appropriate and reasonable method'.

[29] PIPC Guidelines 3-3 I states in relation to Art 11 (2) of the Rules (from Prof Miyashita's translation): 'A recognition based on an international framework concerning the handling of personal information" means the one recognized by the competent accreditation organizations based on the agreed rules of the international organizations. This framework requires the continuous measures equivalent to the one that the personal operators have to take. This recognition applies to the certification of APEC CBPRs system of the third party as the importer in the foreign country.'

[30] TrustArc (formerly TRUSTe), APEC Certified Companies < https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list> (as at 5 December 2017).

accreditation in overseas countries by Japan's PIPC is very significant, though its practical effect is as yet limited to facilitating data exports a few businesses in one country, the US.

The reason that this is significant for Japan's adequacy assessment is that it means that, once Japan receives a positive adequacy assessment, any EU-based business can export personal data to a business in Japan, and this business could (subject to compliance with other aspects of Japan's law), re-export the personal data to any APEC-CBPRs compliant business in the USA, irrespective of whether that business was within the EU-US Privacy Shield. The problem with this, from the EU perspective, is that such US businesses (unless they are within the Privacy Shield arrangements), are only committed to comply with privacy standards (the APEC Privacy Framework) which are considerably lower than those of the EU Directive, or the Japanese PPIA, and with no enforcement measures likely to meet adequacy requirements.

It should follow that the EU will take a very critical approach to whether such a 'back door' means of exporting personal data to the USA is consistent with Japan meeting adequacy standards. The GDPR is quite specific that conditions for 'onward transfers' must be taken into account (arts. 44 and 45(2)(a)).

A potential solution to this problem which does not require any legislative amendment. It would require an amendment to the PIPC's Rules so that the exemption of CBPRs-compliant business operators from art. 24 would only apply, in relation to personal information which the business operator had received from an EU controller, to data export recipients to which a positive EU adequacy finding applied (Privacy Shield or otherwise). This would disadvantage few if any parties, and would uphold the purposes of EU adequacy.

Compliance and remedial mechanisms: Too early to know?

In a study of the enforcement of Japan's law in 2014, Prof. F Shimpo and I argued[31] that our study had

> *'... documented the very limited extent to which there is any evidence of any of the possible types of statutory enforcement in relation to the public sector, and in relation to the private sector, and by the co-regulatory systems. So, to put it politely, the puzzle of the effectiveness of Japanese data privacy law remains. The Japanese system does not provide evidence of its effectiveness. Its enforcement mechanisms are not used to any significant extent, and the mechanisms by which most of the enforcement measures work are obscure. The result is a system that asks observers to take it on trust that it is effective.'*

The 2015 amendments to the PPIA strengthened its enforcement provisions, most notably by the creation of a data protection authority (the PIPC) with powers to investigate make recommendations and give directions to businesses (replacing similar powers previously held by individual Ministries in their sectors). The PIPC was given no powers to issue administrative penalties or fines. Some criminal penalties were added (arts. 82-88), but none exceed a trivially small maximum fine of ¥1M (US$9,900), which in comparison with current EU fines looks as though a couple of zeros are missing. There are still no explicit provisions under PPIA for data subjects to seek financial compensation, either from the PIPC or from the courts. Prior to the 2015 amendments, Japanese courts had refused to provide tort law remedies, including compensation, for breaches of the PPIA, and it is not clear that the

[31] G. Greenleaf and F. Shimpo ' The puzzle of Japanese data privacy enforcement ' *International Data Privacy Law*, Volume 4, Issue 2, 1 May 2014, Pages 139–154 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3086490> ; see also G Greenleaf *Asian Data Privacy Laws* – Trade and Human Rights Perspectives (OUP, 2014) Chapter 8 'Japan – The Illusion of Protection'.

position is now different.[32] To a large extent, the 2015 enforcement powers are a continuation of the limited enforcement position since 2003, but with the PIPC now playing a central role.

While these slightly expanded enforcement powers, and the PIPC's role, exist in theory, most only came into effect since May 2017, so there has as yet been no time for the Japanese system to demonstrate they extent to which they will actually be used, and that the failures of past enforcement have been reversed. Whatever may be the position in a few years time, given Japan's demonstrably poor record of enforcement in the past, it must be seriously questioned whether the Directive's requirements of 'a good level of compliance', 'support and help to individual data subjects' and 'appropriate redress to the injured parties' have as yet been met. Perhaps they are not capable of being met given the continuing remedial weaknesses. Should an adequacy assessment simply take these matters on trust of future stronger enforcement?

Note: In Part II of this article, some similar issues in relation to the adequacy assessment of South Korea will be considered. This article was written before the Article 29 Working Party's 'Adequacy Referential (Updated)' (November 2017) was available, but it makes no substantive difference to this article. It will be discussed in Part II.

[32] For details, see G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 258-9.