

Japan's data privacy laws compared with laws in other Asian countries, and globally

Graham Greenleaf

UNSW Faculty of Law, Sydney

JSPS Visiting Fellow, Meiji University

Prof Horibe Study Group 11/11/2012

1

Outline

1. Have data privacy laws spread *globally*?
2. Whose *standards* do these laws follow?
 - Which standards do *Asian* countries follow?
3. How do Japan's laws compare
 - with laws in other Asian countries?
 - with international standards?

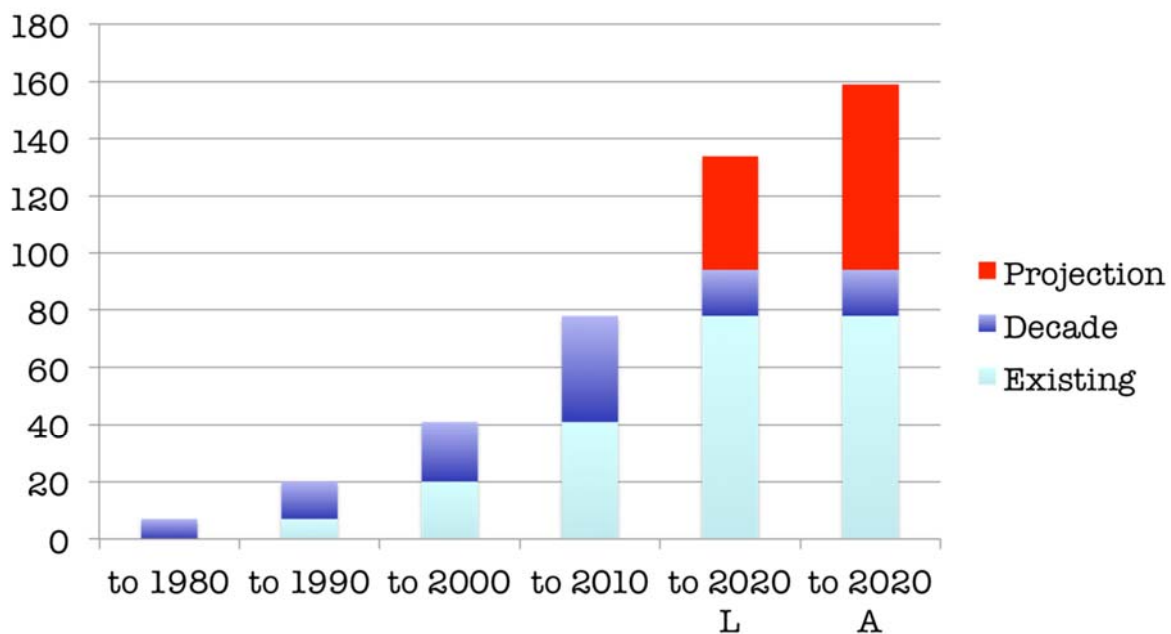
2

Globalisation of data privacy laws

- **94** 'countries' now have data privacy laws
 - 97 if add public sector only (US + Thailand + Yemen)
- **By decade, the growth is accelerating**
 - 1970s: 8
 - 1980s: 13 (21)
 - 1990s: 21 (42)
 - 2000s: 36 (78)
 - 2010s: 16 in 3 years (94)
 - **BY 2020 = between 125 and 150 laws**
- **Will soon include all significant countries**

3

Jurisdictions with data privacy laws – by decade



94 jurisdictions with private sector data privacy laws by Nov 2012, with projections to 2020 (linear = 135; accelerated = 160)

Recent Acts & current Bills

Acts (2012)

- Ghana
- Nicaragua
- Philippines
- Singapore
- Yemen
- South Africa
- Brasil
- Thailand
- Nigeria
- Kenya
- + at least 10

Bills (current)

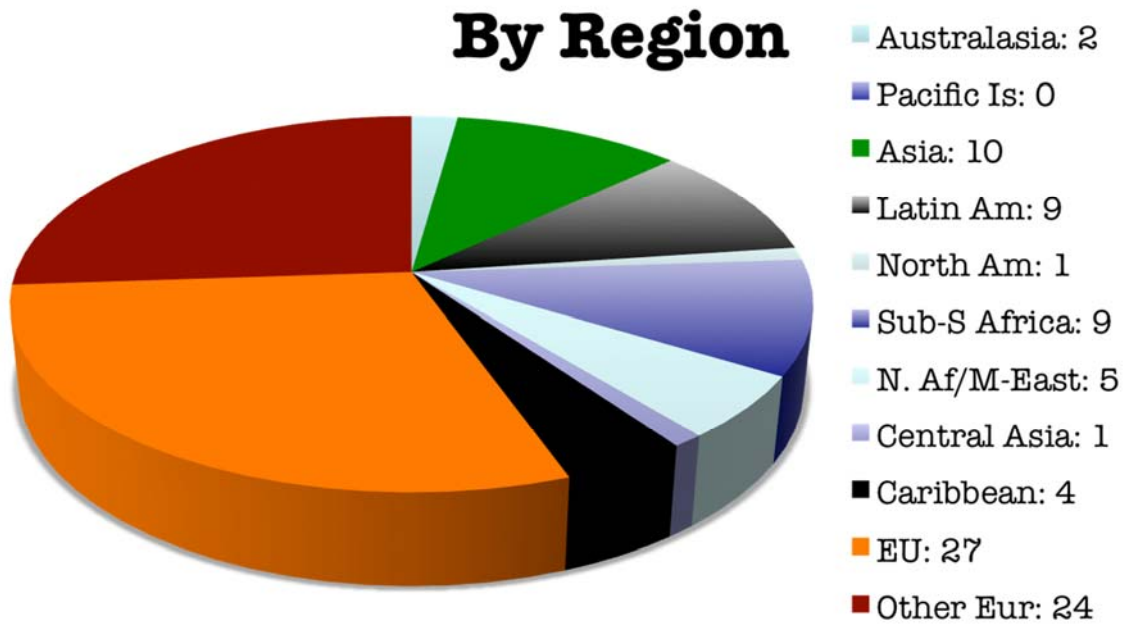
5

Geographical distribution

- **43/94** jurisdictions are outside Europe
 - 51 European = EU: 27 (all); Other European: 24
 - 43 Non-European = Asia: 10; Latin America: 9; Sub-Saharan Africa: 9; N.Africa/M-East: 5; Caribbean: 4; Australasia: 2; N. America: 1; Central Asia: 1; Pacific: 0
- Geo-political implications from 2015 on:
 - *Majority* of 100+ laws will be outside Europe
 - A global web of data protection laws
 - Most of these laws will have data export restrictions, not only the European laws

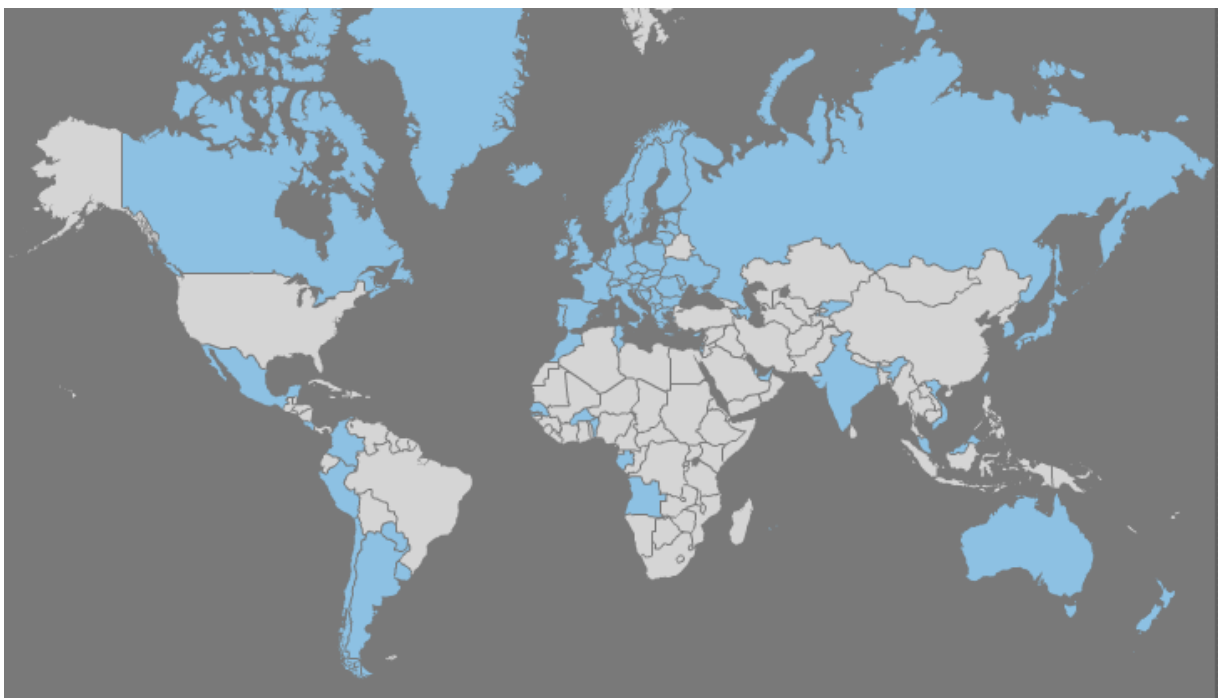
6

94 Jurisdictions with data privacy laws



94 laws: 51 **European**, 43 outside Europe (Nov 2012)

94 countries with (private sector) data privacy laws



What standards are enacted globally? – ‘OECD / basic’ or ‘European’ ?

1. Must first answer: ‘what are *European* data privacy standards?’
2. Approach: What is required by the EU Directive but not required by the OECD Guidelines?
3. Identified the 10 key differences as ‘European standards’
4. Examined 33/37 non-European laws (as at Dec. 2011) against these 10 criteria

9

10 ‘basic’ OECD/CoE standards (*OECD & Council of Europe 1981*)

‘Data privacy law’ = Law implementing most of these principles

1. *Data quality* – relevant, accurate, & up-to-date
2. *Collection - limited*, lawful & fair; with consent or knowledge
3. *Purpose specification* at time of collection
4. *[Notice of purpose* and rights at time of collection (implied)]
5. *Uses & disclosures limited to purposes specified* or compatible
6. *Security* through reasonable safeguards
7. *Openness* re personal data practices
8. *Access* – individual right of access
9. *Correction* – individual right of correction
10. *Accountable* – data controller with task of compliance

10

10 'European' standards

EU Directive & CoE 108+Add. Protocol

1. Has an independent DPA; (*enforcement*)
2. Allows remedies via the courts; (*enforcement*)
3. 'Border control' restrictions on data exports;
4. 'Minimality' in collection (relative to purposes);
5. General 'fair and lawful processing' requirement;
6. Must notify DPA, and allow some 'prior checking';
7. 'Deletion': Destruction or anonymisation after use;
8. Additional protections for sensitive data;
9. Limits on automated decision-making;
10. 'Opt-out' of direct marketing uses required.

An 'adequate' law = one implementing *most* of these 11

Do non-European laws share Euro-standards?

1. 19/33 countries had *at least* 7 Euro-standards.
2. Six standards were *commonplace*
 1. 'border control' data exports (28);
 2. sensitive data extra protection (28);
 3. Deletion after use expires (28);
 4. Individual right to sue in court (26);
 5. minimum collection (26);
 6. separate Data Protection Authority (25).
3. ***Conclusion: Europe's most important standards are now global standards***

Influence of 'European standards' ?

EU 27 100%	CoE 24 90%
ROW 43 70%	USA 1 ?

1980s 'OECD basic' standard is no longer the global standard

Have APEC's privacy standards had any effect?

- APEC privacy principles = "OECD Lite"
 - They are mainly weak versions of the OECD principles
 - They added no new principles *based on Asian laws*
- APEC Framework adds 3 principles:
 - 'Preventing harm' (I); and 'Choice' (V) have not been adopted as principles in *any* non-Euro laws
 - 'Accountability' re data exports (IX) is adopted in Mexico and Singapore, and may be adopted in Australia and New Zealand; Canada's provision pre-dates APEC
- APEC principles have had minimal effect



10 data privacy laws in Asia

15

11 Asian data privacy laws *Dated from privacy sector coverage*

- | | |
|---------------------------|----------------------------------|
| 1. Pre-1995 public sector | (2010) |
| 2. Hong Kong (1995) | 10. India's 'Rules' (2011) |
| 3. Taiwan (1995) | 11. S.Korea #2 (2011) |
| 4. S.Korea (2001) | 12. Hong Kong #2 (2012) |
| 5. Japan (2003) | 13. Philippines (2012) |
| 6. Macau (2006) | 14. Singapore (2012) |
| 7. Malaysia (2009) | <i>Revisions (#2) in Taiwan,</i> |
| 8. Taiwan #2 (2010) | <i>Korea and Hong Kong =</i> |
| 9. Vietnam consumer | <i>stronger laws</i> |

Table comparing 10 laws (extract)

<i>Jurisdictions¹</i>	<i>HK</i>	<i>IN</i>	<i>JN</i>	<i>KR</i>	<i>MA</i>	<i>MY</i>	<i>PH</i>	<i>TW</i>	<i>SN</i>	<i>VN</i>	<i>Os</i>
<i>OECD & CoE108 content principles</i>											
Collection 'limits' ('not excessive')	0	0 ²	0	0	0	0	0	0	0	X	9
Collection by lawful means	0	X	0	0	0	X	0	0	0	X	7
Collection by fair means	0	X	0	0	0	X	0	0	0	X	7
Collection with knowledge	0	0	?	0	0	0	0	0	0	0	9
Data quality – relevant, accurate, complete & up-to-date	0	X	0	0	0	0	0	0	0	0	10
Notice – Purpose of collection 'specified' by time of collection	0	0	0	0	0	0	X	0	0	0	10
Uses limited to purpose of collection, with consent or by law	0	0	0	0	0	0	0	0	0	0	11
Disclosure limited to collection purpose, with consent or by law (or stricter)	0	0	0	0	0	0	0	0	0	0	10
Secondary uses and disclosures only allowed if compatible (or stricter)	0	0	0 ³	0	0	X ⁴	0	0	0	0	10
Secondary purpose 'specified' at change of use (or stricter)	X	0	0	0	0	0	0	?	0	X	7
Security safeguards ⁵ – 'reasonable'	0	0	0	0	0	0	0	0	0	0	11
Openness re policies re personal data	0	X	0	0	0	X	X	0	0	X	6
Access to individual personal data	0	0	0	0	0	0	0	0	0	X	9
Correction of individual data	0	0	0	0	0	0	0	0	0	0	9
Accountable data controller	0	0	0	0	0	0	0	0	0	X	10
<i>Total for OECD/CoE principles /15</i>	14	11	14	15	15	11	13	15	15	8	13

17

Results of comparison of 10 Asian jurisdictions

1. Most have implemented OECD 'basic' principles (Av. 13/15 per Act)
2. 'European' principles are widely implemented in Asia (av. 5.8/10 per Act)
 - Right of court action (8); deletion (8); minimal collection (7); border control data exports (6); sensitive data (6); separate Data Protection Authority (6)
3. Ten additional non-OECD principles are shared by at least 3/10 Acts in Asia

18

Asian comparison (cont)

4. Strongest privacy principles: Korea & Macau
 - Vietnam, India, Malaysia & Japan weakest
5. Broadest range of enforcement mechanisms: Macau & Korea
 - Japan, India & Malaysia have the narrowest
 - Only Japan & Malaysia have no right to court action
6. The new Korean legislation is the strongest & most inventive in Asia

19

Deficiencies of Japan's laws from a European perspective

- What is a 'European perspective' ?
 1. The standards used to assess 'adequacy'.
 2. The standards used to assess non-European applications to accede to Council of Europe data protection Convention 108.
- These two standards are very similar
- They require a law implementing *most* of the 10 'European' standards
 - But there is always some flexibility applied

20

Problems with the principles in Japan's laws

1. Exemption for small businesses

- How does a data subject know if a business has less than 5,000 files? (A2(3)(5))

2. Allowing non-related disclosures by website notice + 'opt-out' (A23(2))

3. No 'minimal collection' requirement

4. No deletion after use completed

- Right to request deletion not enough (A27(1))

21

Problems with principles (2)

5. No 'opt-out' from direct marketing

- 'Anti-spam law' is not enough

6. No 'border' limits on data exports

- 'Due diligence' in supervising trustees is not enough

■ Result: Japan's law = 'OECD basics'

- Its law ignores what Europe looks for
- Most Asian laws are now well beyond OECD

22

Problems with enforcement of Japan's laws

1. No independent agency (DPA)
2. No right to sue in court for breaches
 - None in Act; none otherwise (2007 case)
3. No effective system of offences
 - No offences or fines simply for breaches
 - Ministries do not give orders, so no breaches
4. No significant alternative remedies
 - Privacy Mark does not provide remedies

23

Problems with enforcement (2)

5. Not enough transparency
 - No visible decided cases & remedies resulting

Result: Weakest enforcement in Asia

- Where is the evidence the EU seeks?
 1. a 'good level of compliance'
 2. 'appropriate redress to injured parties'
 3. 'support and help to individual data subjects'

24

Further details

- Greenleaf, G ['The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108'](#) *International Data Privacy Law*, Vol. 2, Issue 2, 2012
- Greenleaf, G ['Global Data Privacy Laws: 89 Countries, and Accelerating'](#), + periodic updates to [Global data privacy laws Table](#) on home page
- [Graham Greenleaf's Web Pages – 2012](#) at [<http://www2.austlii.edu.au/~graham/>](http://www2.austlii.edu.au/~graham/) has links to both above documents