The Global Trajectory of Data Privacy Laws: Asia-Pacific Impact

Graham Greenleaf
UNSW Faculty of Law
Emerging Challenges in Privacy Law Conference, Monash, 23/2/2012

Quiz: A ‘European thing’?

1. How many countries (+ independent jurisdictions) have a ‘data privacy law’ covering most of their private sector?
   - 40+/ 50+/ 60+/ 70+/ 80+/ 90+/ 100!!
2. How many outside Europe? Where?
   - 10+/ 30+/ 50+/ 100!!
3. How many non-Europeans have laws comparable to ‘European standards’?
   - None / A few / Most / All

Unexpected answers? (1)

- Q1 – 88 ‘countries’ have data privacy laws
- 90 if you add the US and Thailand (public sector only)
- By decade, the growth is accelerating
  - 1970s: 8
  - 1980s: 13
  - 1990s: 21
  - 2000s: 35
  - 2010s: 12 in 2 years (linear growth = 50)
- A pessimistic projection, is 125 laws by 2020; an optimistic projection (modest acceleration) is 150
88 countries with (private sector) data privacy laws

Map created by interactive maps: http://www.ammap.com

Unexpected answers? (2)

- **Q2: 37/88 jurisdictions outside Europe**
  - EU: 27 (all); Other European jurisdictions: 23 (3 not: Turkey, Belarus & Georgia - little growth potential)
  - Asia: 8; Latin America: 8; Sub-Saharan Africa: 8; N.Africa + M.East: 6; Caribbean: 4; Australasia: 2; N. America: 1; Central Asia: 1
- **Significant geo-political implications:**
  - Almost all growth will now occur outside Europe
  - By 2014-16, the majority of laws will be outside Europe
  - When most of the commercially significant world has such laws, the focus will not be European ‘data exports’

100+ data privacy laws by 2015? (private sector)

This map adds 14 countries with known official data privacy Bills
Map created by interactive maps: http://www.ammap.com

Who’s missing?

- **Trade-significant absent countries:**
  - Brazil; S.Africa; Indonesia; Nigeria; Turkey
  - Most have bills in various states of advancement
  - And of course China and the USA… the ‘outliers’
- **China**
  - No-one knows which way China will go
  - In 2007 an EU-style national law looked to be in favour
  - Since then a profusion of local and sectoral laws, guidelines, criminal laws, tort law etc
The USA - conclusions

1. No practical prospects of a comprehensive data privacy law passing the US Congress - lobbying against is too powerful
2. The sum total of US private sector laws probably don’t meet the OECD Guidelines, even if applied nationally
3. Constitutional necessity (mainly 1st Amendment) may prevent US private laws ever meeting EU standards of restrictions on disclosure, use or collection
   - case law inconclusive but Sorrell v IMS Health 2011 very negative
4. Result is that Europe (and the ROW) cannot compromise with US standards without capitulation
5. Europe/ROW has to politely accept that US laws are different, then politely enforce their own laws against US companies wherever they are ‘within reach’

Q3: ‘European standards’?

- For Q3 we first have to answer ‘what are European data privacy standards’?
- Approach: What requirement are in the Directive and CoE 108 but not in the OECD Guidelines or APEC Framework (even as recommendations)
  - These differences = distinctly European standards
  - Then identified the 10 key differences; ignored others

10 distinctive European requirements

1. Has an independent DPA;
2. Allows recourse to the courts;
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.

Do non-European laws share these standards?

- Method: Examined 35/37 laws (with assistance) against these 10 criteria
  - Omits St Lucia, Gabon, Paraguay, St Vincent & Grenadines
- Results:
  - 10/33 have at least 7 Euro-standards; 13 have 9+/10
  - The average occurrence of the 10 standards is 22/33 laws
    - By country the average is 7/10 standards present
  - Seven standards were commonplace (>75% laws)
    - ‘border control’ data exports (28); sensitive data protection (28); deletion (28); recourse to courts (26); minimum collection (26); and a DPA (25)
  - Least common are automated decision-making controls (13); and prior checking (17)
Most and least ‘European’

- The laws with 8-10 Euro-features:
  - Peru; Uruguay; Burkina Faso; Senegal; Angola; Argentina; Macau; S.Korea; Mauritius; Costa Rica; Benin; Cape Verde; Columbia, Tunisia
- The laws with 1-4 Euro-features:
  - India; Israel (out-of-date?); Armenia; Bahamas; Japan; Chile; Vietnam
- One third of the laws are in the middle (5-7)
- ‘Euro-scores’ say nothing about effectiveness of laws
  - ‘Adequacy’ is a different (tough) question: Burkina Faso (10); Argentina (9); compared with Canada (7); New Zealand (6)
  - Effectiveness is not a Q of ‘law in the books’; investigation of actual enforcement is needed, and that is a different study
  - No direct implications for whether ‘adequate’ or suitable for CoE accession

Influence? - Implications

- Correlation is not causation
  - Repeated independent invention is logically possible
  - Raab shows indirect DPA networks of influence
  - Emulation of ‘world standards’ is powerful as ‘adequacy’
- Does it create a rebuttable presumption?
  - Likely that European standards have been the second most significant influence on privacy laws
- The ‘family’ origins of data privacy laws
  - Shared OECD/CoE standards from 1981 have had the most influence on privacy laws world-wide

Common elements in OECD & CoE (Euro) standards

1. Data quality – relevant, accurate, up-to-date (OECD 8; CoE 5(c), (d))
2. Collection – limited, lawful and by fair means; with consent or knowledge (OECD 7; CoE 5(a))
3. Purpose specification at time of collection (OECD 9; CoE 5)
4. Notice of purpose and rights at time of collection (OECD ambiguous; APEC stronger; CoE not explicit but implied)
5. Uses & disclosures limited to purposes specified or compatible (OECD 10; CoE 5(b))
6. Security through reasonable safeguards (OECD 11; CoE 7)
7. Openness re personal data practices (OECD 12; CoE 8(a))
8. Access – individual right of access (OECD 13; CoE 8(d))
9. Correction – individual right of correction (OECD 13; CoE 8(c),(d))
10. Accountable – data controller accountable for implementation (OECD 14; CoE 8)

Compare OECD & APEC

- The OECD Guidelines have been influential
  - OECD / CoE 108 core principles are commonplace
  - But nothing not found in the European instruments
- APEC Framework adds 5 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 recommended by law reform bodies in Australia and New Zealand; Canada’s provision pre-dates APEC
- Result: APEC principles have had minimal effect
Can CoE 108 be globalised?

- Q: Do/will ubiquitous data privacy laws make a global agreement either (I) possible or (II) useful?
  - Will see the answer to both (I) and (II) is ‘Yes’
- Candidates:
  - (i) A new UN Treaty from scratch is unrealistic
  - (ii) Europe has no need to negotiate some OECD-Lite 1980s compromise with APEC and the USA
  - (iii) A global patchwork quilt of CBPRs will not happen
  - (iv) That leaves CoE data protection Convention 108 as the only contender: How realistic is 108 globalisation?

CoE Convention 108

- Convention 108 + Additional Protocol = Directive (approx.)
  - 2001 Protocol added essential missing parts (DPA required, data export restrictions, access to courts)
  - Without Protocol, Conv 108 = ‘Euro standards’
- 43/47 CoE member states have ratified Conv 108 and have laws
  - 31 have also ratified Additional Protocol
  - This is a very good start for a global agreement

Decision to globalise 108

- A 23(1) has allowed accession by non-CoE-member-states since 1981
  - Requires unanimity of contracting states for a non-European state to be invited to accede
- 2008: Consultative Committee (CC) of Conv 108 finally decided to activate 23(1)
  - Agree to consider requests from countries ‘with data protection legislation in accordance with Conv. 108’
  - Prompted by resolution of DPA meeting in Montreux
  - 2009: EU’s ‘Stockholm Program’ included world-wide promotion of Convention 108

Why the Additional Protocol is essential

- What if a non-European state is allowed to accede only to the Convention?
  - No obligation to have a DPA or provide access to the Courts
  - No obligation to prevent onward flows of data
  - All other members are still obliged to allow data exports to it, unless they explicitly derogate
- A ‘back-door’ defeat of Euro-standards
- Problem solved if country either (i) already has all of the Additional Protocol elements or (ii) accedes to Protocol as well
  From a Civil Society perspective, non-European accession is only desirable if also to the Protocol
Accession procedures & standards

- 2011 brief Note from CoE Treaty Office:
  1. Non-Euro country should write requesting accession
  2. Euro Members are consulted first: unanimity
  3. Non-Euro Members (none yet) then given time to raise objections
  4. If no objections, invitation sent
  5. Non-Euro country must comply before acceding
- Most key questions remain unanswered...

Problems with accession procedures & standards

1. Clarity needed on compliance with Additional Protocol standards
   § Bureau claims that compliance with both is necessary
2. What evidence is required that a country meets CoE standards?
   § Purely formal or substantive assessment? Cannot be purely formal - some countries have DPAs in the laws but not in fact
   § CoE is only used to dealing with democratic countries
3. How can EU 'adequacy' findings/ Opinions be used in accession procedures?
   § Key difference is that 'adequacy' is aimed at protection of Europeans; CoE must be concerned with country's citizens

Problems with accession procedures & standards (2)

4. What role will the Consultative Committee play in accession?
   § Peers? (countries); Experts?; DPAs like WP29?
5. How can citizens of non-Euro countries enforce their rights?
   § Non-Euro citizens cannot utilise A8 ECHR - powerless
   § Could the CC be empowered to accept 'complaints'?
6. Procedures to enforce compliance over time?
   § CoE 'modernisation' may include 'follow-up' procedures

Advantages of accession to non-Euro countries

- Guarantees free flow of personal data from 43 Euro countries
  - Directive guarantees nothing; and only 27
- CoE (+AP) accession means EU adequacy is unlikely to be denied
  - It should be a higher standard than adequacy; and is an international commitment, also likely to be faster
- Avoids need to make decisions about exports to other countries (21/28 have data export laws)
- Voluntary entry into a treaty as an equal partner
  - Some non-Euro states resent 'adequacy' as an imposition
Advantages of non-Euro accession to Euro countries

- Creates free flow of personal data obligations on all non-Euro Parties
  - Adequacy doesn’t create reciprocal obligations
  - 21/28 non-Euro laws have data export laws
- Consolidates global position of Euro standards
  - Increases consistency with Directive obligations
  - Advantages for Europe-based companies in consistent global standards
  - Improves capacity to resist pressure from USA

The Uruguay accession

- July 2011: Council of Ministers invited Uruguay to accede
  - Based on 2 page Opinion of Consultative Committee (CC)
  - CC Opinion was based on materials sent to sent to 43 Member representative of CC: (i) favourable EU WP 29 Opinion; (ii) the Act; and (iii) request letter from Uruguay
  - Only 14 bothered to confirm ‘no objection’, 29 silent
  - CC then adopted Opinion by written procedure
- Q: Will Uruguay accede to Additional Protocol?
  - Does it already comply?; Not addressed in CC Opinion
  - But invitation to Uruguay was to accede to both instruments

Unsatisfactory aspects of the Uruguay accession

- What procedures will be adopted when there is no WP29 Opinion to rely on?
  - Will Expert assessment be commissioned (as the EU Commission does, when a WP29 Opinion is absent)?
  - ‘Adequacy’ is not the correct standard for accession
- CC Opinion does not address reality of protection to Uruguay citizens
  - Fortunately WP29 Opinion does so to some extent
- No Civil Society or other non-State input
  - A CoE accession affects the citizens of all other countries that are Parties: they should have input

Will CoE 108 become a global standard?

- As yet, more promise than reality
  - CoE 108 Bureau is confident of ‘a long list’ of accessions
  - Mexico has announced its intention
- A lot of things may go wrong
  - CoE 108 Bureau has done little to publicise advantages and ‘sell’ accession
  - Civil Society may strongly oppose accessions if standards are not kept high
- But getting it right has major benefits
  - The only realistic prospect of a (high) global standard
  - This would improve both trade and human rights
Further details

- 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/> has links to both above documents