



Global proliferation of data privacy laws: *Future implications and European influences*

Professor Graham Greenleaf AM

Professor of Law & Information Systems,
UNSW Australia

Asia-Pacific Editor, *Privacy Laws & Business International Report*

Privacy Laws & Business 28th Annual International Conference

St John's College, Cambridge, 6 July 2015

Overview

- A. The global expansion of data privacy laws
- B. Global data privacy standards **from below**:
The standards applied in laws outside Europe
- C. The 'Goldilocks' standard: What is feasible?
- D. Global data privacy standards **from above**:
How successful are the 4 competing standards?
- E. The UN Special Privacy Rapporteur 2015-18:
How can they advance a global standard?

A. The global expansion of data privacy laws (1973-2015)

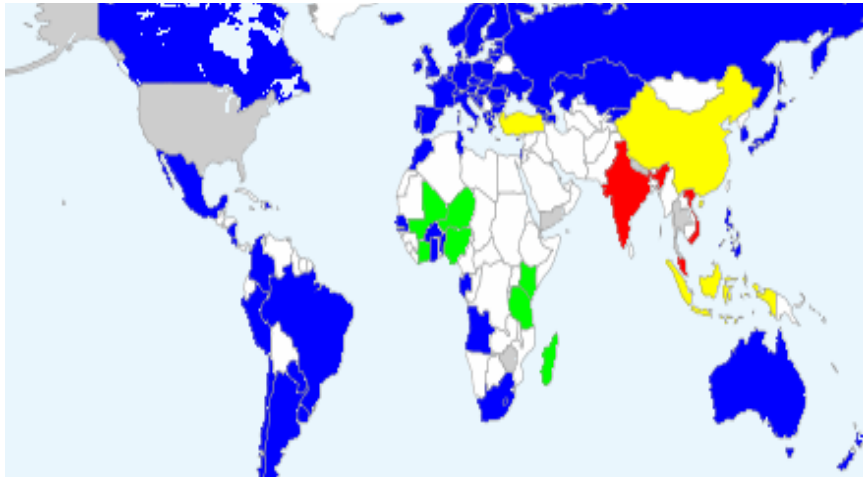
- **109 countries now have a data privacy law** (June 2015)
 - 10 additions in last year; some are major (eg South Africa) and some minor (small African & Caribbean countries)
 - Some only recently in force (eg Malaysia, Singapore; many African)
- 2014 is the first time the majority of global privacy laws (56/109) are from **outside Europe**.
 - And more countries have such laws than those that do not
- Global ubiquity of data privacy laws is occurring
 - At least 24 more countries currently have **official Bills**
 - Growth of new laws globally is still **accelerating**
 - Also many stronger “2nd generation” **revised** laws (eg In Asia Pacific - Korea, Hong Kong, Taiwan, Australia; Japan Bill)

3

24 Bills for new data privacy Acts

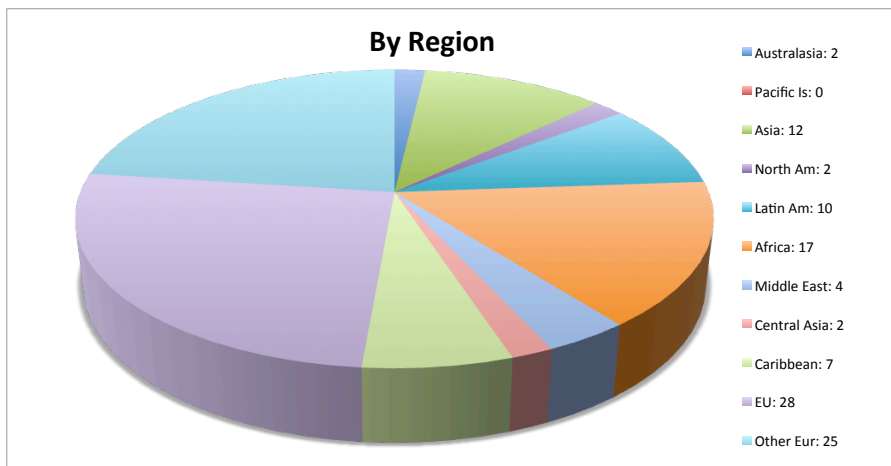
- | | |
|----------------------|-------------------------------|
| 1. Antigua & Barbuda | 13. Jamaica |
| 2. Barbados | 14. Kenya |
| 3. Bermuda | 15. Mauritania |
| 4. Brazil | 16. Niger |
| 5. Cayman Island | 17. Nigeria |
| 6. Chad | 18. Qatar |
| 7. Dominica | 19. Saint Kitts and Nevis |
| 8. Ecuador | 20. Swaziland |
| 9. Ethiopia | 21. Tanzania |
| 10. Falkland Islands | 22. Thailand (private sector) |
| 11. Grenada | 23. Turkey |
| 12. Honduras | 24. Uganda |

Global map of data privacy laws (to be amended to remove Brazil! + add more Bills)



BLUE = ALL; GREY = PUBLIC; RED = ALL PRIVATE; YELLOW = MOST PRIVATE; GREEN = BILL ONLY

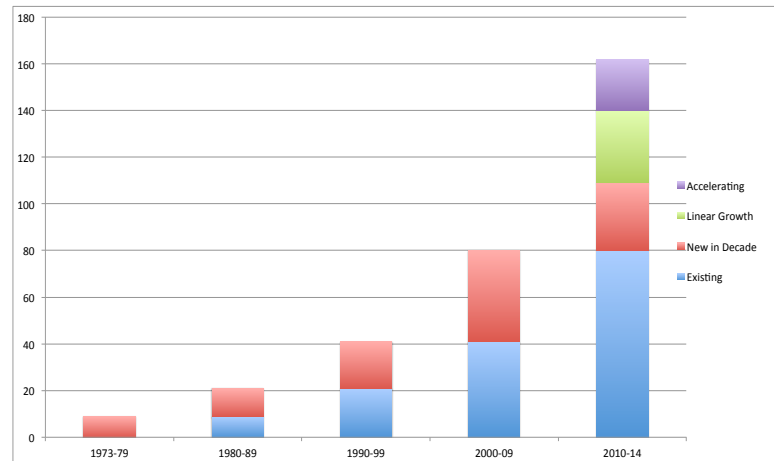
Regional spread of data privacy laws



109 laws: 53 European, 56 outside Europe (June 2015)

6

Jurisdictions by decade: *Diffusion to ubiquity*



**109 jurisdictions with data privacy laws by June 2015,
with projections to 2020 (linear = 139; accelerated = 160)**

7

What is the scope of the 109 laws?

- Globally, 98/109 cover both **private & public sectors**
 - Only 6 are Private sector only (Vietnam, Singapore, Malaysia; India, Qatar & Dubai SEZs)
 - More private-sector-only laws may emerge from e-commerce/ consumer privacy laws (eg Turkey; China; Indonesia)
 - 5 are Public sector only (Thailand, Nepal, Zimbabwe, Yemen, + USA which also has many non-comprehensive private sector laws)
- Globally, 99/109 laws have a **separate Data Protection Authority (DPA)**
 - Asia unusual in *having laws without DPAs* (Taiwan, India, Vietnam + Japan for the moment; also China and Indonesia)
 - But, this 'Ministry-based model' is in decline in Asia: new DPAs in Korea, Malaysia, Singapore, Philippines (TBA) + Bill in Japan; likely in India.
 - Also unusual in having *non-independent DPAs* (Singapore, Malaysia)

B. Which privacy principles are implemented in non-European laws?

1. Approach: Do Asian laws implement OECD 'basic' standards or 'European' standards?
2. 'OECD standards' = 10 principles (also in EU)
3. 'European standards' = What is required by the EU Directive but **not** required by the OECD Guidelines?
4. I identified the 8 key differences in principles (+2 re enforcement) as 'European standards' (next slide)
5. In 2011, I found that 33 non-European laws averaged almost 7 'European' principles (out of 36 existing)
6. APEC Framework (2004): principles are 'OECD Lite' + 3 US-influenced, but none of the 8 'European' principles

10 'European' standards

EU Directive (1995) & CoE 108 +Add. Protocol (2001)

Main differences between the OECD Guidelines and the EU Directive:

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

On average, data privacy laws outside Europe (2011) included 6 or 7 of these principles, in addition to the 'basic' OECD principles

Which privacy principles are implemented in non-European laws? (2)

- In 2015, what standards do the now-56 non-European laws implement?
 - Comprehensive study not yet completed: but the position is clear enough:
 1. The 20 new post-2011 laws generally strongly adopt 'European standards'.
 2. Numerous '2nd Generation' laws from the previous 36 strengthen their principles (eg Hong Kong; S.Korea, Taiwan; Japanese Bill)
 - The 2015 average will be at least as strong as the 2011 average of 7/10 European standards.

Regional study (2014) of principles implemented in Asian laws

Table 17.2 Comparison of general principles and collection principles

	Source	CN	HK	IN	JN	KR	MA	MY	PH	TW	SN	VN
<i>General principles</i>												
'Fair and lawful processing' general requirement	EURO	√	X	X	X	√	√	√	√	√	X	X
'Personal data' defined in terms of identifiability	OECD	√	√	√	√	√	√	√	√	√	√	√
Specified contact at controller (accountable data controller)	OECD	√	√	√	√	√	√	√	√	√	√	√
'Privacy officer' required	ASIA	X	X	X	X	√	X	X	X	X	X	X
Onus of proof on controller	ASIA	X	X	X	X	X	√	X	X	X	X	X
Openness re policies on personal data	OECD	√	√	X	√	√	√	X	X	√	√	X
Published privacy policy	ASIA	√	√	√	X	√	√	√	X	√	√	√
'Preventing harm'	APEC	X	X	X	X	X	X	X	X	X	X	X
'Choice'	APEC	X	X	X	X	X	X	X	X	X	X	X
<i>Collection principles</i>												
Collection—'limited' (only)	OECD	X	X	X	√	X	X	√	√	X	X	√
Collection—'minimum necessary' for purpose	EURO	√	√	√	X	√	√	X	X	√	√	X

Part of one of five Tables comparing principles

Asian laws: Basic (OECD) principles implemented

- Implementation of 8 OECD/basic principles in 11 Asian laws:
 - collection limitation (11/11); data quality (9/11); purpose specification (10); use limitation (9); security safeguards (11/11); openness (10); individual participation (10); and accountability (11/11) (to give them their OECD names).
 - On average, each principle is implemented in slightly more than 10/11 jurisdictions. Asian experience therefore bears out the argument that these principles are the universally accepted basis of data privacy laws.
- The shortcomings from full implementation of these basic principles in Asia differ between countries:
 - China (data quality; use and disclosure limitations; individual participation); India (data quality); Philippines (purpose specification; openness); Japan (new disclosures merely by notice); Malaysia (secondary uses inconsistency).

Asian laws: European principles implemented

- Implementation of 8 'European' principles in 11 Asian laws:
 - data export restrictions based on destination (5/11); minimal collection (7/11); 'fair and lawful processing' (5/11); deletion (8/11); sensitive data protections (5); automated processing controls (2/11); prior checking (4/11); and direct marketing opt-out, or opt-in (8/11).
 - On average, each principle is implemented in more than 5 of the 11 jurisdictions, and each jurisdiction implements almost four principles.
 - Asian data privacy laws sit 'halfway' between OECD and European principles.
- Implementation of the three 'APEC principles' in 11 Asian laws:
 - Two of them, 'preventing harm' and 'choice', have not been implemented in any data privacy law in Asia.
 - The third, 'data export accountability', is arguably implemented in Singapore, but it can equally be argued to be *sui generis* and much stronger than APEC.
- **Conclusion:** Asian data privacy laws are strongly influenced by European privacy principles, though not as strongly as in other regions (Africa & Latin America). APEC principles have no influence.

C. The 'Goldilocks' standard: What is feasible and acceptable?



How do you make porridge that is 'just right'?
What global privacy standard would meet the 'Goldilocks standard'?

The 'Goldilocks' standard: How to make porridge, or standards (2)

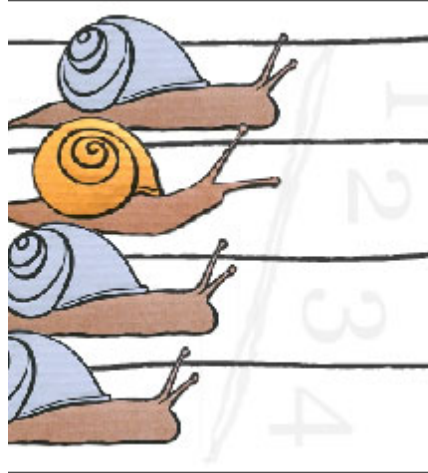
1. **You must start with the ingredients you have.**
 - 109 existing laws have an inertia; any global standard must approximate what they require
2. **It must meet the goals of a healthy lifestyle.**
 - Goal 1: Provide sufficient privacy protection
 - Goal 2: Allow free flow of personal data in return
3. **It must not be too hot, or no-one can eat it.**
 - Too hot if standards are so high that most States must amend their laws
4. **It must not be too cold, or it will be avoided.**
 - Too cold if most States must surrender their citizens' privacy in exports to other States with too low privacy protections allowed to be Parties.
5. **But if it is 'just right', everyone will want it.**
 - The 'just right' balance entices States to voluntarily accept a global standard, and their citizens not to oppose it.

Conclusion: To have a Porridge Party, your dish must be 'just right' for the maximum number of Parties you want to Treat.

D. Top-down progress toward a global standard: 'The Snail Race'

Place your bets in the global privacy sweepstakes!!

1. OECD Guidelines 1980 + post-2013 'adherence'
2. EU Directive 1995 + 'adequacy'
3. CoE Convention 108 + 'globalisation'
4. UN ICCPR 1966 + new impetus post-Snowden



Not eligible to race (Stewards' scratchings)

African Union data protection & cyber security Convention 2014

- No provision for non-African states to adhere, or be declared 'adequate' – so **not a global Convention**
- No ratifications yet; but procedures have started
- 15 required to be in force
- Potentially important: 54 AU members could join; has 'European' standards
- *A pathway to continent-wide cooperation with CoE 108?*

APEC Cross-border Privacy Rules (CBPR)

- 21 potential members
- Only the USA is a full member yet; benefits uncertain
- 3 have started procedures to join (Japan, Mexico, Canada), but this may take years
- No 'interoperability' with other systems exists or likely; some common procedures with EU BCRs
- **Not a global standard or procedure – 'interoperability' is not the future**

1. OECD Guidelines 1980 + post-2013 non-member 'adherence'

- 1980 OECD Guidelines: 34 members, 32 have laws except Turkey & USA (part private sector)
- 1980 standards (largely unchanged by 2013 revision) – lower than most of the 109 laws
 - Too 'cold' a standard to encourage adherence
- 2013 revision allows non-OECD-members to 'adhere' to Guidelines (to obtain free flow benefits) – **none** known to have done so

Conclusion: OECD Guidelines have become largely irrelevant to establishing a global standard

2. EU data protection Directive 1995 + 'adequacy' findings

- 28 EU members + 3 EEA members + 22 other CoE members and territories with similar standards
- 'Adequacy' mechanism has only added a handful of non-European countries since 1999 (none since 2012)
 - Canada; Argentina; Israel; Uruguay; New Zealand; US 'Safe Harbor'
 - Could the EU Commission have done more (eg Mexico; Korea; in Africa)?
- EU Directive's 'adequacy' standard is similar to what many countries enact ('half-way between OECD & European standards')
 - Will the 'adequacy' standard of the proposed EU Regulation be 'too hot' or 'just right' to encourage non-European countries to meet it?
- 'Adequacy' has problems as a globalisation mechanism: appears unilateral; does not guarantee free flow *from* 'adequate' countries

Conclusion: While the EU Directive has in practice encouraged 'European standards', it is not a long-term mechanism for globalisation; it needs to work in conjunction with CoE 108

3. CoE Convention 108 + 'globalisation' accessions

- 46/47 CoE members have ratified Convention 108 (Turkey absent)
 - 44 signed and 35 ratified the Additional Protocol
- Since 2010, CoE has actively encouraged non-European accessions:
 - Uruguay is the only completed accession
 - Morocco (2013), Mauritius (2015) accessions near-complete
 - Senegal (2015) invited to accede; Tunisia shortly
- Main advantage: Starts with 50+ members, and now growing
 - almost 50% of those possible
- Problem: Citizens of non-European States have no individual redress mechanism (contrast A.8 ECHR and ECtHR cases)

CoE Convention 108 + 'globalisation' accessions (2)

- **Current** CoE 108+Protocol standards and accession requirements are similar to many of the 109 laws ('half-way to European standards')
 - Can CoE speed up accessions without lowering standards ('too cold')? (eg Mexico, Korea, NZ, Canada – soon Japan, Australia??)
 - CoE Consultative Committee and Council of Ministers both need to ensure that standards are not lowered. NGO vigilance required.
- CoE **Modernisation** process is at final draft stage (CAHDATA);
 - its provisions are moderately stronger than at present, but would require only minimal legislative changes (if any) to many non-European laws.
 - its non-European accession standards are unchanged, allowing flexibility in application, but oversight by the Convention C'tee.
 - States can accede for (initially) only some of their territory (eg China in respect of Hong Kong and Macau SARs)

CoE Convention 108 + 'globalisation' accessions (3)

Conclusions:

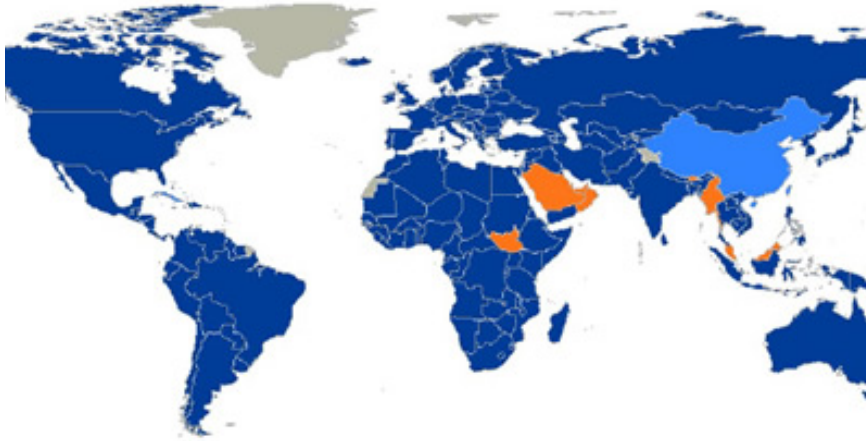
- CoE Convention 108, both now and after 'modernisation', will be similar to the standards already adopted in many of the 109 laws;
- CoE 108 has preferable globalisation mechanisms: States voluntarily become Parties; they obtain mutual benefits (free flow of data); they are then Parties to future changes.
- CoE 108 will continue to be a possible and feasible global standard (neither too hot nor too cold).
- Active cooperation between the CoE and the EU could ensure that European standards were more visibly and speedily adopted as the global standard

4. UN ICCPR 1966 + new impetus post-Snowden

- UN's International Covenant on Civil & Political Rights 1966 (ICCPR), A. 17
 - World's most widely adopted privacy obligation
 - UNHRC 'General Comments' (1989) on A.17 interpret it as requiring many (but not all) basic data protection rights
 - Most of Latin America, Africa, Canada & Australasia have ratified 1st Protocol, allowing individual ICCPR 'communications' to the UNHRC
 - UN General Assembly Guidelines for Regulation of Computerized Data Files (1990) recommend adoption of the full set of basic data privacy principles
- Adoption of a new UN data privacy Treaty from scratch is very unlikely and would be likely to have low standards

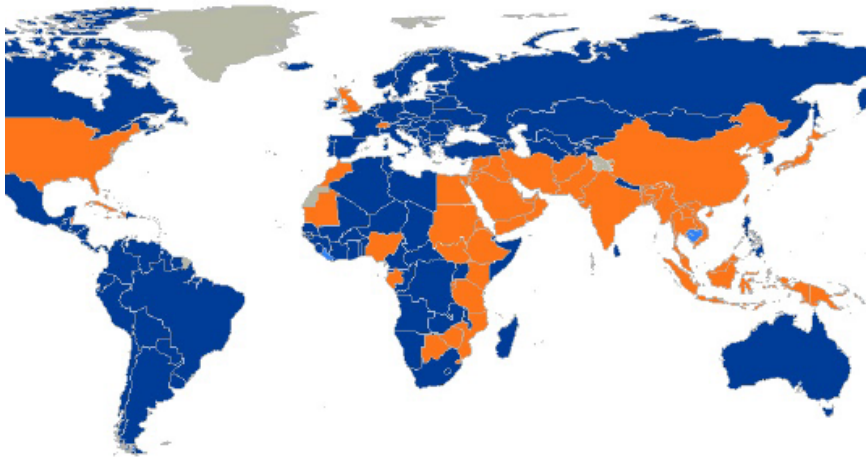
Can the new UN Privacy Rapporteur bring the UN from behind?

Ratifications of the ICCPR



Almost all countries have ratified the ICCPR, except a few in Asia.

ICCPR 1st Optional Protocol ratifications



Most of Latin America, Africa, Canada & Australasia allow individual ICCPR 'communications'

E. The new UN Privacy Rapporteur – Their data privacy mandate

- UN GA Resolution 28/16 ‘The right to privacy in the digital age’ (Dec 2014)
 - Calls on States to provide ‘an effective remedy’ to those affected by ‘unlawful or arbitrary surveillance’
 - Encouraged HRC to identify ‘principles, standards and best practices’ for protection of privacy.
- UN Human Rights Council Resolution (April 2015) decided to appoint a Special Rapporteur for 3 years
 - Mandate includes ‘(c) To identify possible obstacles to the ... protection of the right to privacy, to identify, exchange and promote principles and best practices at the national, regional and international levels, and to submit proposals and recommendations to the [HRC] ...’
 - Rapporteur to be appointed by 1 July 2015

The new UN Privacy Rapporteur – Advancing a global standard

Consistent with the HRC’s mandate, the Rapporteur could consider recommending to the HRC (and indirectly to the CoE):

1. That the standards of CoE Convention 108 are now international ‘best practice’, consistent with and implied by ICCPR A.17.
2. That States should consider applying to ratify Convention 108, once their laws meet that standard.
3. That the CoE should require non-European countries who wish to accede to Convention 108 to also accede to ICCPR 1st Protocol.
4. That the HRC should accept ‘communications’ (complaints) from individuals in Member States that are parties to both (a) the ICCPR 1st Optional Protocol and (b) Convention 108, that Convention 108 is not observed.
 - This would place citizens of non-European states that have ratified Convention 108 in a position closer to European citizens (who have the benefit of ECHR A. 8).

The new UN Privacy Rapporteur – Advancing a global standard (2)

5. That (if found necessary for 4 above) a new 3rd optional Protocol should be added to the ICCPR:
 - a. Affirming that the standards of CoE Convention 108 are implied by ICCPR A.17.
 - b. Accepting that citizens of the State may make communications to the HRC as in the 1st Protocol if there is non-compliance with Convention 108 standards.

The ICDPPC recommended in 2013 a similar 3rd Optional Protocol adopting an international privacy standard.

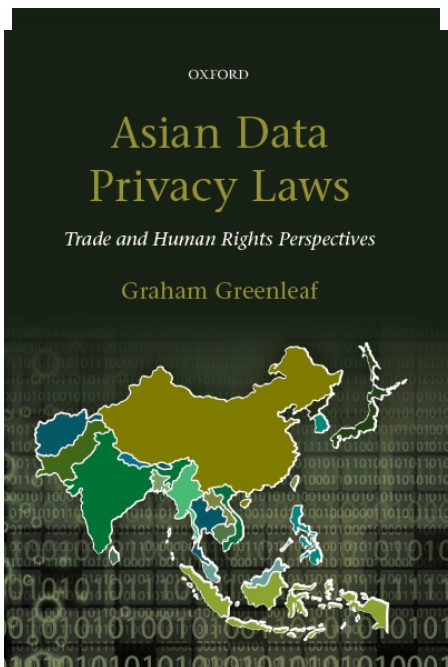
Conclusion

- All paths to a global privacy instrument which protects individual privacy while allowing flows of personal data between Parties involve complexities and uncertainties.
- In the 40+ years since the first data privacy laws, national progress (bottom-up) has been rapid and is accelerating, but an international instrument (top-down) has been slow to emerge.
- An international agreement should respect and reflect the standards that have emerged from national legislation.
- Council of Europe Convention 108 is the best (perhaps the only) prospect for a global agreement, if other parties decide to collaborate. It is a realistic and desirable option.

References

- G Greenleaf (General Editor) *International Privacy Law Library* (on WorldLII) <http://www.worldlii.org/int/special/privacy/>
- G Greenleaf 'Global data privacy laws 2015: 109 countries, with European laws now in a minority' (2015) 133 *Privacy Laws & Business International Report*, 14-17.
- G Greenleaf 'Global data privacy laws 2015: DPAs and their organisations' (2015) 134 *Privacy Laws & Business International Report*, 16-19.
- G Greenleaf 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2 (2) *International Data Privacy Law*, <http://ssrn.com/abstract=1960299>
- G Greenleaf *Asian Data Privacy Laws* (OUP, 2014)- see Chs 2 and 17-20; Ch 1 available at <http://ssrn.com/abstract=2514972>
- G Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2013) 23(1) *Journal of Law, Information & Science* <http://ssrn.com/abstract=2280877>
- G Greenleaf & M Georges 'The African Union's Data Privacy Convention: A Major Step Toward Global Consistency?' (2014) 131 *Privacy Laws & Business International Report*, 18-21
- For other papers see my SSRN page at <http://ssrn.com/author=57970>

31



32

WorldLII International Privacy Law Library

News & Announcements

- [Click](#) to publish decisions of data protection and privacy authorities in WorldLII's International Privacy Law Library
- [User guide to WorldLII's International Privacy Law Library](#) (2 July 2014)

Search:

Search: Databases Catalog & Websearch Law on Google

Last updated: 11 September 2014

Databases

Case Law

- [Austrian Information Commissioner Case Notes 2011](#) (WwLII)
- [Austrian Privacy Case Summaries 2012](#) (WwLII)
- [European Commission Article 29 Working Party Conclusions and Recommendations 2002](#) (WwLII)
- [Federal Privacy Commissioner of Australia Case Notes 2011](#) (WwLII)
- [Federal Privacy Commissioner of Australia Complaint Determinations 2002](#) (WwLII)
- [Federal Privacy Commissioner Case Studies 2002](#) (WwLII)
- [European Personal Information Directive National Committee Cases 2002](#) (WwLII)
- [Malaysian Office for Personal Data Protection Case Notes 2012](#) (WwLII)
- [New Zealand Privacy Commissioner Cases 2012](#) (WwLII)
- [New Zealand Privacy Commissioner Cases 2006](#) (WwLII)
- [Office of the European Data Protection Officer 2012](#) (WwLII)
- [Office of the European Data Protection Officer 2011](#) (WwLII)
- [Office of the Privacy Commissioner for Personal Data, Hong Kong - Administrative Appeal Board Case Notes 2012](#) (WwLII)
- [Office of the Privacy Commissioner for Personal Data, Hong Kong - Administrative Appeal Board Case Notes 2011](#) (WwLII)
- [United Kingdom Information Commissioner's Office 2011](#) (WwLII)
- [United Kingdom Information Commissioner's Office 2006](#) (WwLII)
- [United States Federal Trade Commission Privacy Case Summaries 1998](#) (WwLII)
- [United States Health Information Privacy Regulation Agreements and Case Summaries 2002](#) (WwLII)

Other Cases Concerning Privacy and Surveillance Issues (WwLII)

Law Journals, Commentary and Resources

- [Austrian Privacy Law Resources](#) (WwLII)
- [ECHR and UNHRC](#) (WwLII)
- [EU Data Protection and Human Rights Report 2006](#) (WwLII)
- [International Privacy Law Resources](#) (WwLII)
- [Privacy Law and Data Breach: 1992](#) (WwLII)
- [Privacy Laws and Business International Report 1992](#) (WwLII)

Other Law Journal Articles Concerning Privacy and Surveillance Issues (WwLII)

Law Reform Publications

- [Law Reform Publications Concerning Privacy and Surveillance Issues](#) (WwLII)

Legislation

- [International Data Privacy Legislation](#) (WwLII)
- [National Privacy Legislation Concerning Privacy and Surveillance Issues](#) (WwLII)

Treaties and International Agreements

- [OECD Privacy Law Recommendation](#) (WwLII)
- [International Conference of Data Protection and Privacy Commissioners Resolutions and Declarations 2000](#) (WwLII)
- [International Data Privacy Conventions](#) (WwLII)
- [Council of Europe Convention 108](#) (WwLII)

Catalog and Websearch

- [Advocacy Organizations](#)
- [Business Organizations](#)