National data privacy laws and international instruments: Is there any point?

Graham Greenleaf
Professor of Law & Information Systems, UNSW

University of Strathclyde, 08/10/13

‘Tell them what you really think…’

1. Are national data privacy laws passé?
2. What about China, India and the USA?
3. What do the opponents of privacy want?
4. Are international agreements irrelevant?
5. Are there better alternatives to laws?
6. Where does that leave us?

What does it mean to say a country has a data privacy law?

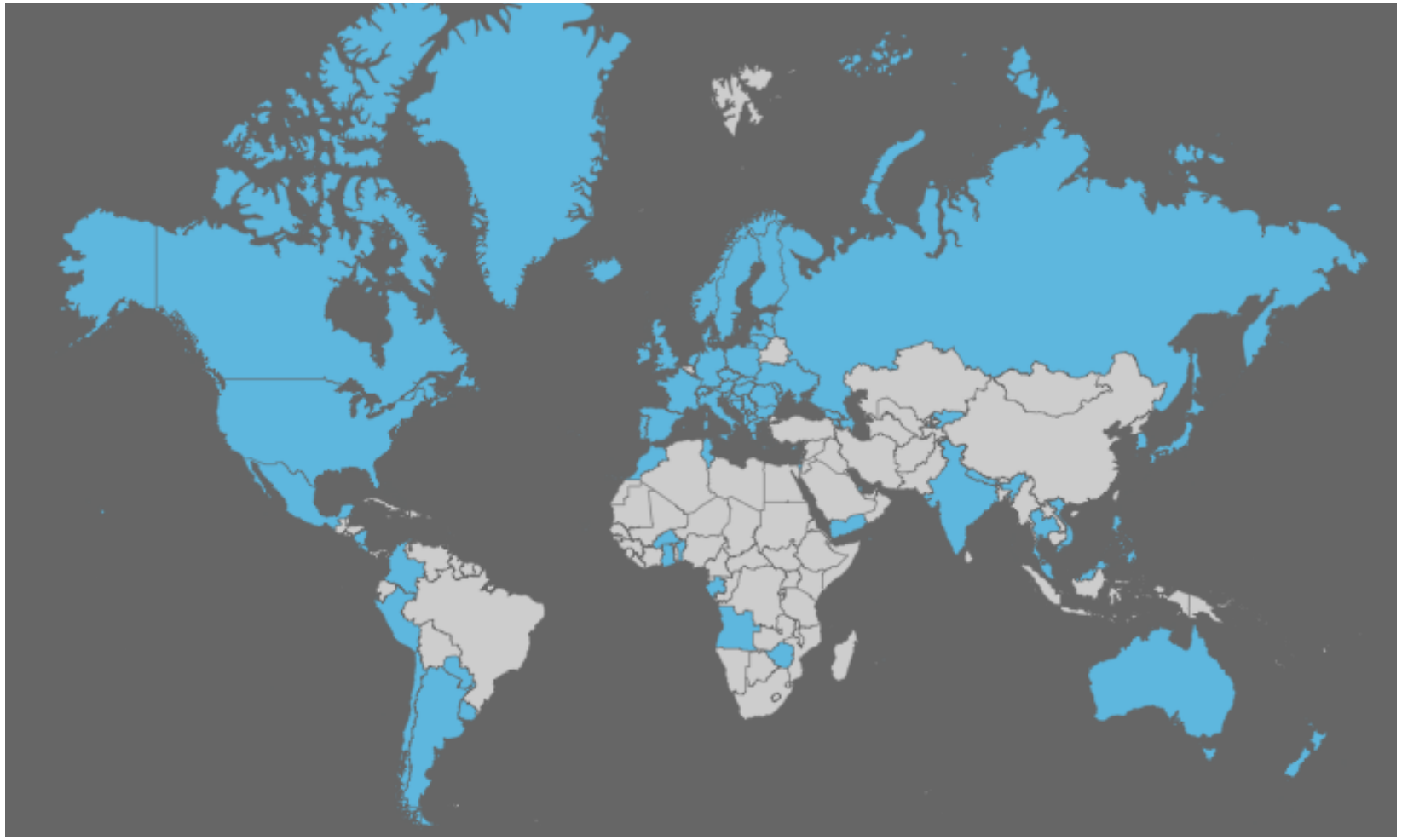
1. What is a **'country'** for this purpose?
   - A separate legal jurisdiction (eg HK, Macau, Jersey, Greenland)
2. What's a **law**?
   - It's a law: not self-regulation or trustmarks
   - Any type of enforcement by law is sufficient, even if ineffective
3. What **scope** must a law have?
   - Must cover (most of) the private sector and/or the public sector
   - Almost all (90%) cover both public & private sectors
4. What **content** must a data privacy law have?
   - 'Most' of the basic principles shared by all international agreements (OECD, CoE, EU and APEC)
   - 11/15 basic principles, including the main ones, is the minimum

'Basic' principles in 10 Asian laws	*HK*	*IN*	*JN*	*KR*	*MA*	*MY*	*PH*	*TW*	*SN*	*VN*	*TTL*
Collection 'limits' ('not excessive')	0	0	0	0	0	0	0	0	0	X	9
Collection by lawful means	0	X	0	0	0	X	0	0	0	0	7
Collection by fair means	0	X	0	0	0	X	0	0	0	0	7
Purpose of collection 'specified' by time of collection	0	0	0	0	0	0	X	0	0	0	9
Collection with knowledge or consent, when from data subject	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	9
Uses limited to purpose of collection, with consent or by law	0	0	0	0	0	0	0	0	0	0	10
Disclosure limited to collection purpose, with consent or by law	0	0	0	0	0	0	0	0	0	0	10
Secondary uses and disclosures only allowed if compatible	0	0	0	0	0	X	0	0	0	0	9
Secondary purpose 'specified' at change of use	X	0	0	0	0	0	0	?	0	X	7
Security safeguards – 'reasonable'	0	0	0	0	0	0	0	0	0	0	10
Openness re personal data policies	0	X	0	0	0	X	X	0	0	0	6
Access to individual personal data	0	0	0	0	0	0	0	0	0	0	9
Correction of individual data	0	0	0	0	0	0	0	0	0	0	10
Accountable data controller	0	0	0	0	0	0	0	0	0	0	10
Total /15	**14**	**11**	**14**	**15**	**15**	**11**	**13**	**15**	**15**	**13**	***13.6***

How many countries now have a data privacy law?

- A: **101** (as at 30 September 2013)
  - 99 in article & Table (see cites) to June 2013
  - + add Kazakhstan and South Africa (unsigned)
- 90/101 cover both sectors
  - 5 Public sector only (Thailand, Yemen, USA, Nepal, Zimbabwe)
  - 6 Private sector only (Vietnam, Singapore, Malaysia; India, Qatar & Dubai SEZs)

Result: 101 countries now have data privacy laws



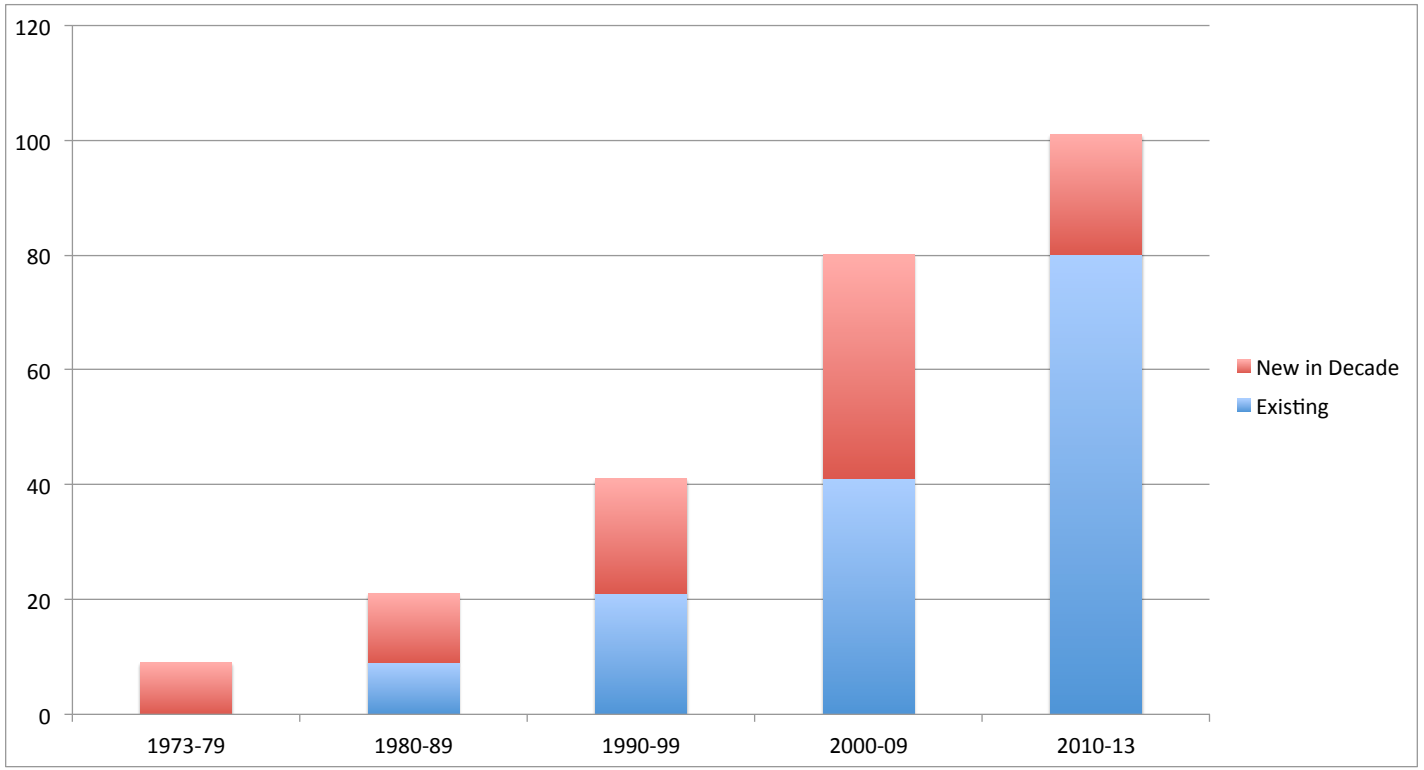
To this map, add Kazakhstan and South Africa – new Acts since mid-2013

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

22 Acts & 19 Bills this decade

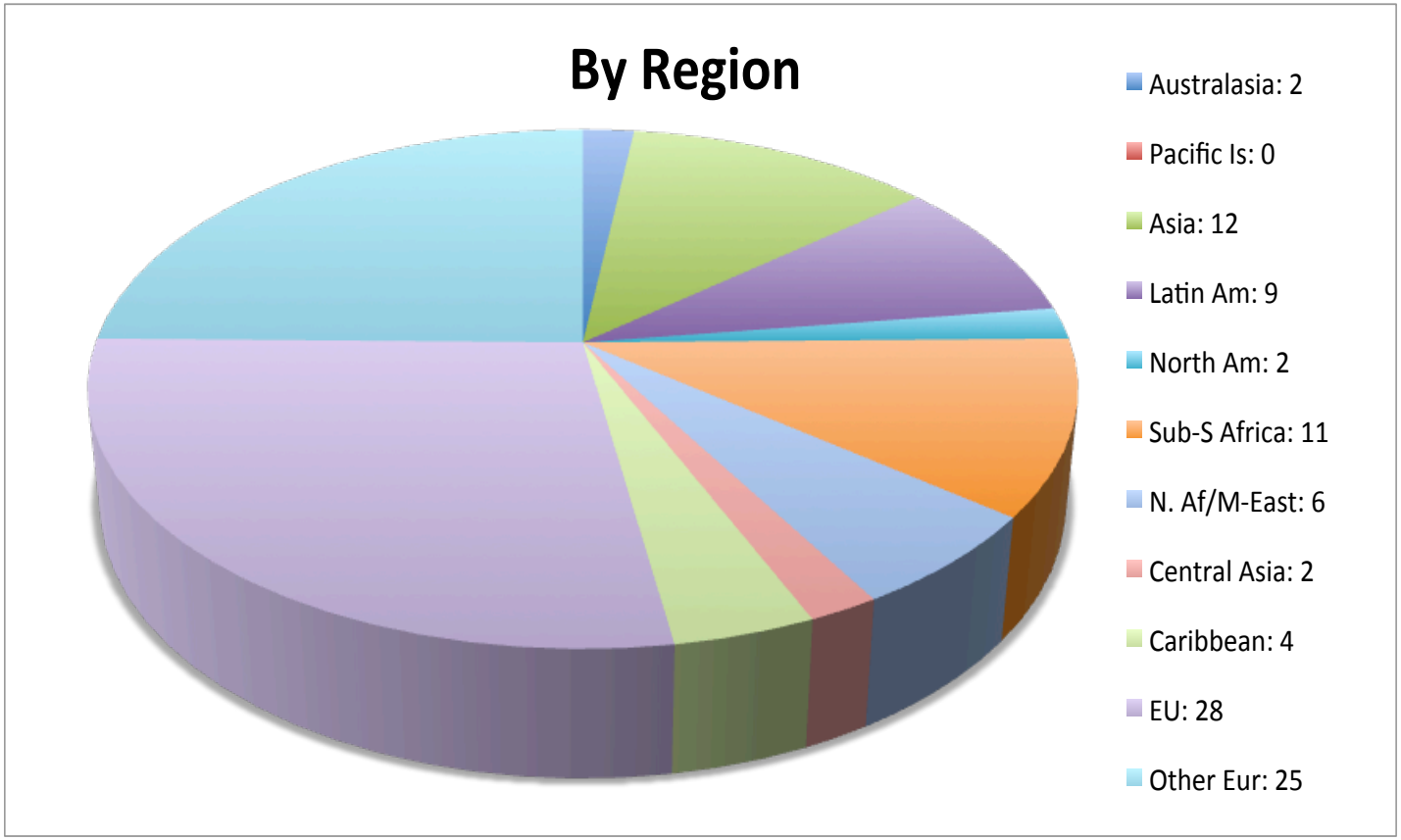
Acts 2010	Acts 2011	Acts 2012	Acts 2013	Bills	Bills
Georgia	Angola	Ghana	Kazakhstan	*Nigeria*	*Thailand*
Faroe Is.	Costa Rica	Nicaragua	South Africa	*Brazil*	*Turkey*
Kosovo	Gabon	Philippines		*Madagascar*	*Tanzania*
Malaysia	India	Singapore		*Kenya*	*Jamaica*
Vietnam	Peru	Yemen		*Falkland Islands*	*Mali*
Mexico	St Lucia	Georgia		*Qatar*	*Niger*
	Trinidad & Tobago			*Ivory Coast*	*+ 5 others in Caribbean*
	Ukraine				

Jurisdictions by decade: *From rare to common*



101 jurisdictions with data privacy laws by August 2013

Regional spread of data privacy laws



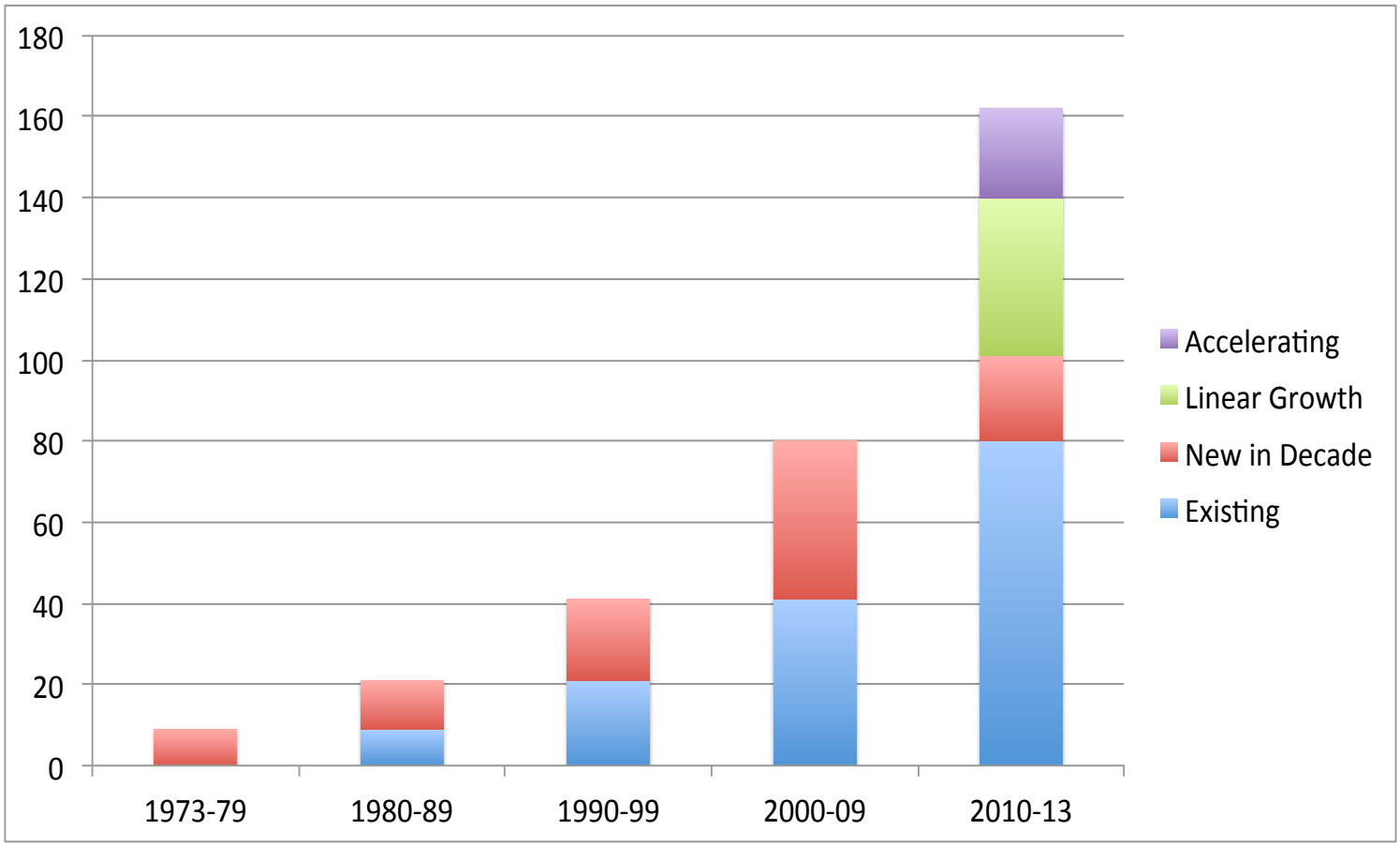
101 laws: 53 European, 48 outside Europe (August 2013)

Countries with no Acts or Bills

Afghanistan; Algeria; Bahrain; Bangladesh; Belarus; Belize; Bermuda; Bhutan; Bolivia; Botswana; British Virgin Islands; Brunei Darussalam; Burundi; Cambodia; Cameroon; Central African Republic; Chad; China; Comoros; Congo, Republic; Congo Democratic Republic; Cuba; Djibouti; Ecuador; Egypt; El Salvador; Equatorial Guinea; Eritrea; Ethiopia; Fiji; Gambia; Guatemala; Guinea; Guinea-Bissau; Guyana; Haiti; Honduras; Indonesia; Iran; Iraq; Jordan; Kiribati; Korea, North; Kuwait; Lao PDR; Lebanon, Lesotho; Liberia; Libya; Malawi; Maldives; Marshall Islands; Mauritania; Micronesia; Mongolia; Mozambique; Myanmar; Namibia; Nauru; Oman; Pakistan; Palau; Palestine; Panama; Papua New Guinea; Rwanda; Samoa; Sao Tome and Principe; Saudi Arabia; Sierra Leone; Solomon Islands; Somalia; Sri Lanka; Sudan; Suriname; Swaziland; Syria; Tajikistan; Timor Leste; Togo; Tonga; Turkmenistan; Tuvalu; Uganda; United Arab Emirates; Uzbekistan; Vanuatu; Vatican; Venezuela; Zambia

China and Indonesia already have significant IT sector laws

Jurisdictions by decade: *Diffusion to ubiquity*



101 jurisdictions with data privacy laws by August 2013, with projections to 2020 (linear = 139; accelerated = 160)

Consequences of globalisation

- **48/101** jurisdictions with laws are outside Europe
  - No European expansion (all except Turkey, Belarus)
  - In ROW, all regions (except Pacific) are expanding
  - Data privacy laws are everywhere: no longer a 'European thing'
  - Growth is now occur outside Europe; majority by 2014-16
- **Ubiquity** of data privacy laws in countries of economic/ political significance by 2020
  - Most countries with no laws/Bills are in 'the global B team'
  - But are the USA, India and China outliers (private sector)?
- **Data export restrictions** are not limited to the EU, or Europe
  - Export issues will be global, not unidirectional from Europe
- ROW laws **expand, strengthen**, & are increasingly enforced
  - '2nd generation' laws in Korea, Taiwan & HK 2011-12
  - Google enforcement: Korea (TOS) and Macau (Streetview)
  - 50 years of ID numbers is being rolled back in Korea

What standards are enacted globally? – 'Basic' only 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' (next slide)
4. Examined 33/37 non-European laws (as at Dec. 2011) against these 10 criteria
5. **Result:** Average 7/10 'European' factors found
6. Result: Most important factors occurred most often (>75%)
   - Export limits; sensitive data; deletion; court actions; specialist DPA
7. Now 48 laws (not 33) but no apparent significant change

Conclusion: The current 'global standard' is the European standard, to a significant extent (av. 70%)

10 'European' standards

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

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;
6. Limits on **automated decision-making**;
7. 'Opt-out' of **direct marketing** uses required.
8. Has a **separate independent DPA**; *(enforcement)*
9. Allows **remedies via the courts**; *(enforcement)*
10. '**Border control**' data exports restrictions.

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

Invitation to accede to CoE Convention 108 requires similar

Outlier # 1 – China

'Warring States' period (2006-10)

1. 2006/7: Draft *Personal Information Protection Act,* from Institute of Law; private & public sectors; included DPA; EU-influenced
2. Some Provinces have enacted data privacy codes, for consumers
3. Piecemeal laws on money laundering, medical records, insurance, consumer protection and credit reporting
4. 2009-10 Major reforms: Criminal Law and Tort Liability Law

Consistency emerging (2011-13) – private sector only

5. 2011 MIIT (Min. of Industry & Info. Tech.) 'Internet Information Services Regulations', in force 3/12
6. 2012 NPC Standing Committee 'Decision' (a law) on Internet Information Protection, in force 12/12
7. 2013 MIIT Standardization Administration 'Guidelines' on Personal Information Protection in 'computer information systems'
8. 2013 MIIT 'User Data Protection' Regulations'

Result: No national law yet but expanding scope & consistency in principles.

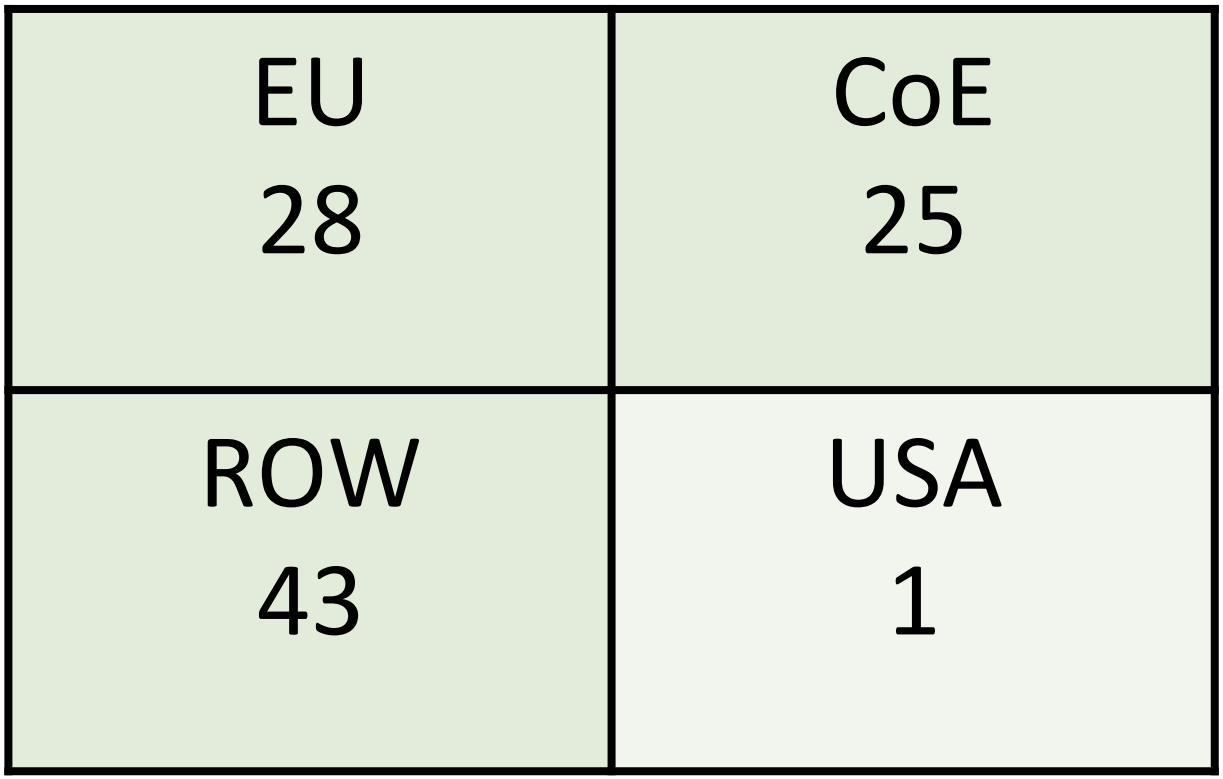
Outlier #2 - India

1. 2011 ‘Rules’ under the IT Act give a private sector law which might not meet OECD-basic criteria
2. India has applied again for EU adequacy – unlikely
3. Government has a draft ‘normal’ privacy law
4. 600M ID numbers issued without any legislation (jammed); success vital to government re-election
5. 23/09/13 – interim Supreme Court order that ID number cannot be mandatory, or for non-citizens
6. Privacy law (to Supreme Court standards) could be the price for (i) the ID number and/or (ii) adequacy

Outlier #3 – The USA

1. US law doesn't & won't meet OECD standards
   - No US law requires companies to use or disclose information only for the purpose it was collected, or minimises collection
   - US Constitution may prevent such laws – uncertain
   - Obama Administration 2012 'Consumer Privacy Bill of Rights' initiative is sub-OECD, does not require legislation
   - OECD-compliant laws are politically impossible in Congress
2. USA does not protect foreigners' privacy
   - PRISM may put most personal data on US servers + communications channels into the hands of the US government
     - All safeguards are overwhelmed or circumvented
   - US says this is only to track 'foreigners' (= us)
3. What does it mean to be 'interoperable' with US standards?
4. The USA is, & is likely to stay, the outlier in global privacy standards

Global **private sector** data privacy map



96 jurisdictions with private sector data privacy laws (+USA)

Thinking of this in EU v US terms grossly over-simplifies

What do opponents of privacy want?

1. Remove legal liabilities from data privacy laws
   - ~~'Accountability' ('due diligence' = no liability) failed~~: EU made it an extra obligation, not an alternative standard
   - 'Risk based' laws are the new favourite: Allow any personal data to be collected; only prevent uses which are shown (somehow) to involve 'risk'
2. Expand 'anonymous' data / contract 'personal data'
   - Coincidence of interests between private sector data aggregation, and governments intent on 'open data'
   - Depends on (i) restricting 'personal data' to 'identification' and not encompassing 'individual interaction'; (ii) pretending that de-identified data cannot be re-identified, or used for interactions.
   - Enables 'data analytics' / 'big data'
3. Destroy data export limitation laws & require 'Interoperability'
   - Result will be data exports to the USA can never be prevented despite low levels of US protection
   - US policy in OECD, CoE, APEC & FTA negotiations to weaken any 'comparable protection' requirements, and require 'free flow'

Are international agreements irrelevant?

1. Revised OECD privacy Guidelines (2013)
2. APEC Cross-Border Privacy Rules (CBPR) (2013)
3. EU Regulation replacing Directive (2014?)
4. 'Modernised' and 'globalised' CoE Convention 108 (2014?)
5. Forget about the UN

Revised OECD privacy Guidelines (2013)

1. Privacy principles frozen at 1980 level (pre-Directive, 33 years ago)
2. Protection of 'uninterrupted and secure' transborder data flows (1980) is removed (hello PRISM & GCHQ!)
3. Recommendation of legislation (1980) is weakened
   - Allows something like APEC CBPR to suffice
   - US First Amendment is also allowed to degrade privacy
4. Non-OECD countries are now invited to adhere to the GLs and implement cross-border 'cooperation' (ie submission re exports)
5. Data exports can only require (undefined) 'accountability'
   - No OECD country can require more, even with non-OECD members
   - No non-OECD 'adhering' country can require more either
   - No longer 'minimum standards' *except domestically*

Purpose: The USA does not care what domestic laws apply (it has lost that fight), provided data exports can't be stopped

APEC CBPR (2013)

APEC's *illusory* Cross-Border Privacy Rules system

1. CBPR only require APEC Framework's (2005) 'OECD-Lite' standards (c. 1980) to be met by *companies* certified under it
2. Only the USA is yet fully engaged (it has no OECD-standard law)
   - TRUSTe is its 'Accountability Agent'; the FTC its enforcement agency; IBM its one certified company
3. APEC CBPR's purpose: to allow data transfers from willing APEC countries to a few US-based certified companies despite weak US laws and remedies
   - Will any other APEC countries use this to obtain transfers?
4. The US then aims for 'interoperability' of this system with non-APEC countries, to circumvent data export restrictions
   - Via new OECD Guidelines, or agreements with EU (like Safe Harbor) or India, or FTAs with others

APEC CBPR is just a smokescreen to protect data exports to the USA

EU Regulation replacing Directive (2014?)

- Reding's bottom line: No reduction from the Directive
- Best chance of a '3rd Generation' set of privacy principles
  - Will be very influential outside Europe
- Key Q remains data export limitations and 'adequacy' / 'interoperability' etc

‘Modernised’ and ‘globalised’ CoE Convention 108 (2014?)

1. Convention (1981) + Protocol (2001) = Directive
2. Since 2012 ‘globalisation’ has started
   - Uruguay; Morocco next; more in the queue
3. ‘Modernisation’ proposals (2012) by Consultative Committee
   - awaiting modification/ approval by ad hoc committee (CAHDATA) of member States + non-European observers
4. Numerous stronger or new principles proposed
   - May equate to EU Regulation ‘3rd generation’
   - May expand ‘personal data’ to include enabling interactions
5. Data exports – replaces ‘adequacy’ requirement with (undefined) ‘appropriate’ protection
   - Risky: A vague term with no Court to interpret it

Possible result: Stalemate

- US technology and State vs global data protection standards
- 'Interoperability' with US standards would be foolish until they improve – maybe forever
- Perhaps the position ought to stay as it is:
  1. Those outside the US respect, but do not accommodate, the inherent limitations in US data privacy protection
  2. No accommodation for the US unwillingness to legislate at all
  3. Inevitable administrative inconvenience for US companies in complying with BCRs, Safe Harbor etc
  4. More frequent problems for US companies (prosecutions, fines, damages) acting outside the USA
  5. Voluntary adoption by many US companies of increasingly global 'European' standards
  6. Increasing isolation of the USA re national laws / global standards

Are there better alternatives to laws?

1. ‘Get over it’ – Abandon privacy as a value
   - Choice: Some do, most don’t
   - Inevitably, the content of privacy as a value *changes*
2. Self-regulation / ISO standards / privacy marks?
   - With pixies or with legal compulsion?
3. ‘Privacy by design’?
   - Yes, but only with legal compulsion
4. Privacy-enhancing technologies (PETs)?
   - Encryption is useless in transactions
5. Counter-surveillance (sousveillance etc)
   - No use against dataveillance

Conclusions

1. Most (not all) people retain privacy as a value, even though its shape shifts
2. No single protective mechanism suffices
3. All protections work better if supported by laws (a) limiting surveillance; & (b) protecting data
4. US companies and government lead those in whose interest is the destruction of privacy
5. National data privacy laws will be ubiquitous
6. They can be subverted by international standards limiting them
7. International standards are worth contesting and strengthening
8. Surveillance & data aggregation is not irreversible
9. The steady global strengthening of national laws & international standards is still the best hope

Further details

- This presentation was supported by the RCUK Centre for Copyright and New Business Models in the Creative Economy (CREATe), AHRC Grant Number AH/K000179/1

- Papers on my SSRN page http://ssrn.com/author=57970 :
  - The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108 (2012)
  - Global Tables of Data Privacy Laws and Bills (3rd Ed, June 2013)
  - Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories (2013)
  - Obama's Privacy Framework: An Offer to be Left on the Table? (2012)
  - Uruguay Starts Convention 108's Global Journey with Accession: Toward a Global Privacy Treaty? (2013)
  - 'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty? (2013)
  - International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement) (2013)
- See also my Web Pages at http://www2.austlii.edu.au/~graham/