100+ Data Privacy Laws: Their Significance and Origins

Graham Greenleaf, UNSW Faculty of Law

2nd Asian Privacy Scholars Conference

Centre for Business Information Ethics

Meiji University, Tokyo, 19 November 2012

Privacy 101 questions

1. What is a ‘data privacy law’ anyway?
2. Where are they, since when, and where from?
3. What are their cumulative implications ?
4. What standards do they follow?
5. Could they be ‘interoperable’?

A simple question …

In Aniane, France, June 2011 – Jim Rule asked:

‘How many countries have data privacy laws now?’

But you have to answer other questions first …

1. What is a ‘country’ for this purpose?
   - A separate legal jurisdiction for the private sector
     - eg HK, Macau, Jersey, Greenland
2. What scope must a law ‘have’?
   - Almost all cover both public & private sectors
     - Public sector only: Thailand, Yemen, USA
     - Private sector only: Vietnam, Singapore, Malaysia; India, Qatar & Dubai SEZs
   - Conclusion: Must cover most of its private sector
     - Vietnam yes; China’s Internet-only law no
     - Australia and Japan yes despite ‘small business’
3. What’s a law?
   - It’s a law: not self-regulation or trustmarks
   - But any type of enforcement by law must be accepted
   - This is only a Q of whether a DP law exists, not ‘adequacy’

More preliminary questions …

4. **What content must a data privacy law have?**
   - Standard texts do not define this
   - Hypothesis: Include 'most' 1981 OECD/CoE principles
     - Eg China's Internet law excluded access/correction - excluded
   - 10-15 OECD Principles, depending on approach
   - Can't require all 15, or too strict
     - Eg no explicit 'openness' principle in 6/10 Asian laws
   - Testing against 10 Asian laws: averaged 13/15
     - Vietnam lowest (8/15), probably should be excluded
     - Malaysia's 11/15 is probably as low as should be accepted
   - Conclusion: Must include minimum 11/15 OECD, including access/correction + some finality principles

10 'basic' OECD/CoE standards *(OECD & Council of Europe 1981)* The 1st Generation Principles

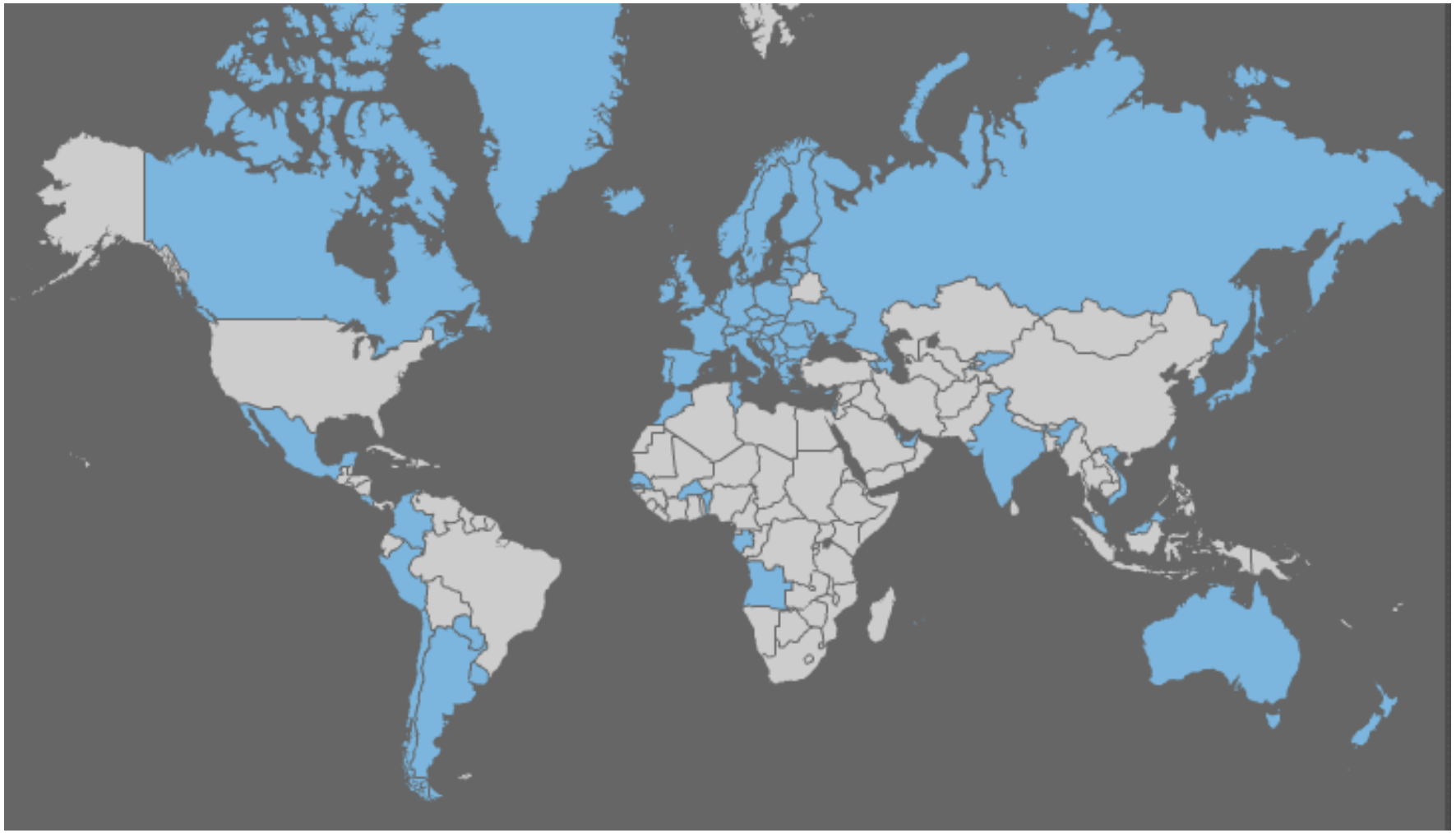
1. *Data quality* – relevant, accurate, & up-to-date
2. *Collection* - limited, lawful & fair; with consent or knowledge
3. *Purpose specification* at time of collection
4. *[Notice* of purpose and rights at time of collection (implied)]
5. *Uses & disclosures limited* to purposes specified or compatible
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

'Data privacy law' = 'Law implementing most of these principles'?

Table comparing 10 Asian laws (extract)

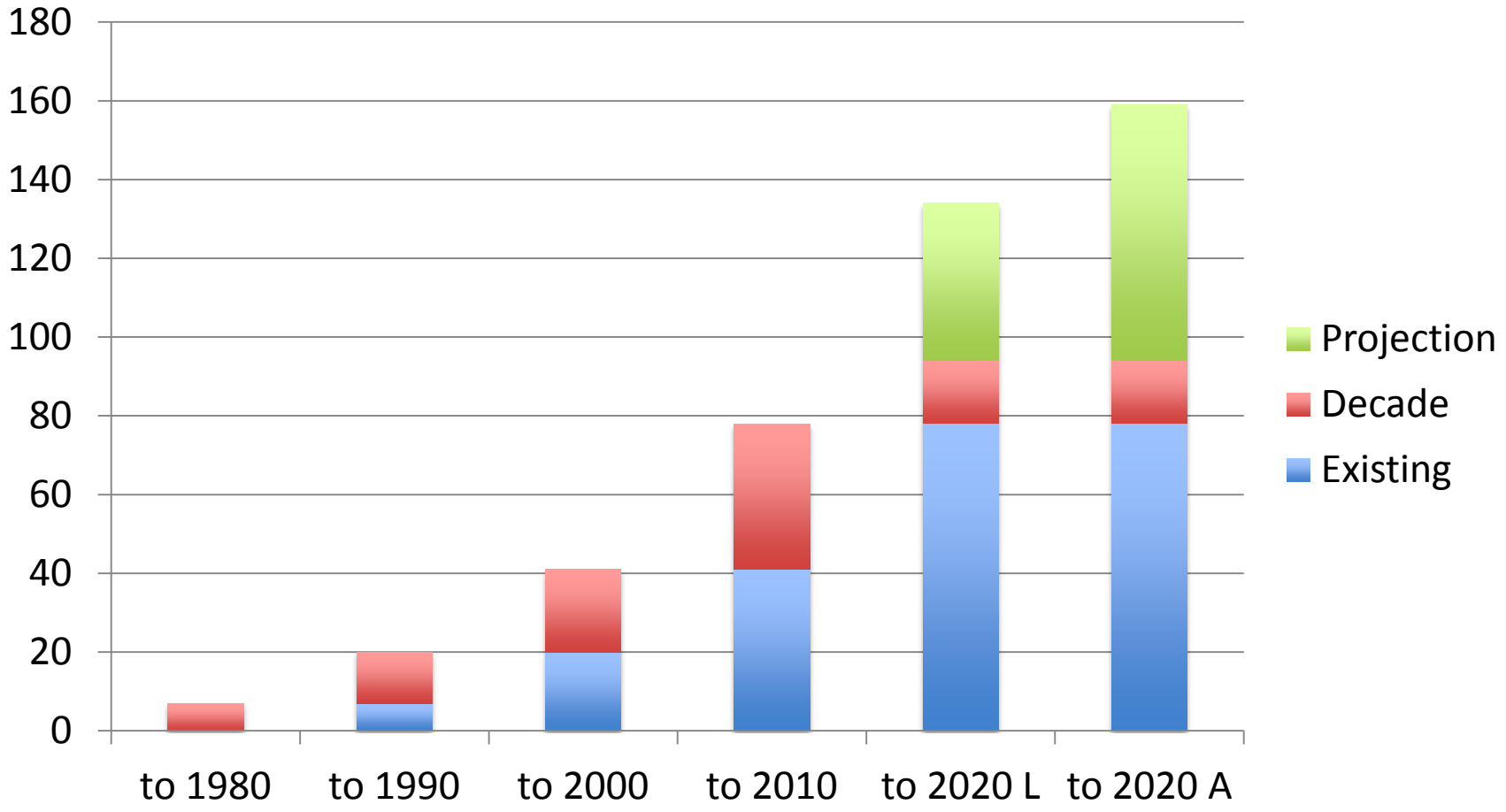
Jurisdictions[1]	*HK*	*IN*	*JN*	*KR*	*MA*	*MY*	*PH*	*TW*	*SN*	*VN*	*TTL*
OECD & CoE108 content principles											
Collection 'limits' ('not excessive')	0	0[2]	0	0	0	0	0	0	0	X	9
Collection by lawful means	0	X	0	0	0	X	0	0	0	X	7
Collection by fair means	0	X	0	0	0	X	0	0	0	X	7
Purpose of collection 'specified' 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 (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	9
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	10
Openness re policies on 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	10
Accountable data controller	0	0	0	0	0	0	0	0	0	X	10
Total for OECD/CoE principles /15	***14***	***11***	*14*	***15***	***15***	***11***	***13***	***15***	***15***	***8***	av13

Result: 94 countries with (**private sector**) data privacy laws



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

Jurisdictions by decade: *Diffusion to saturation*



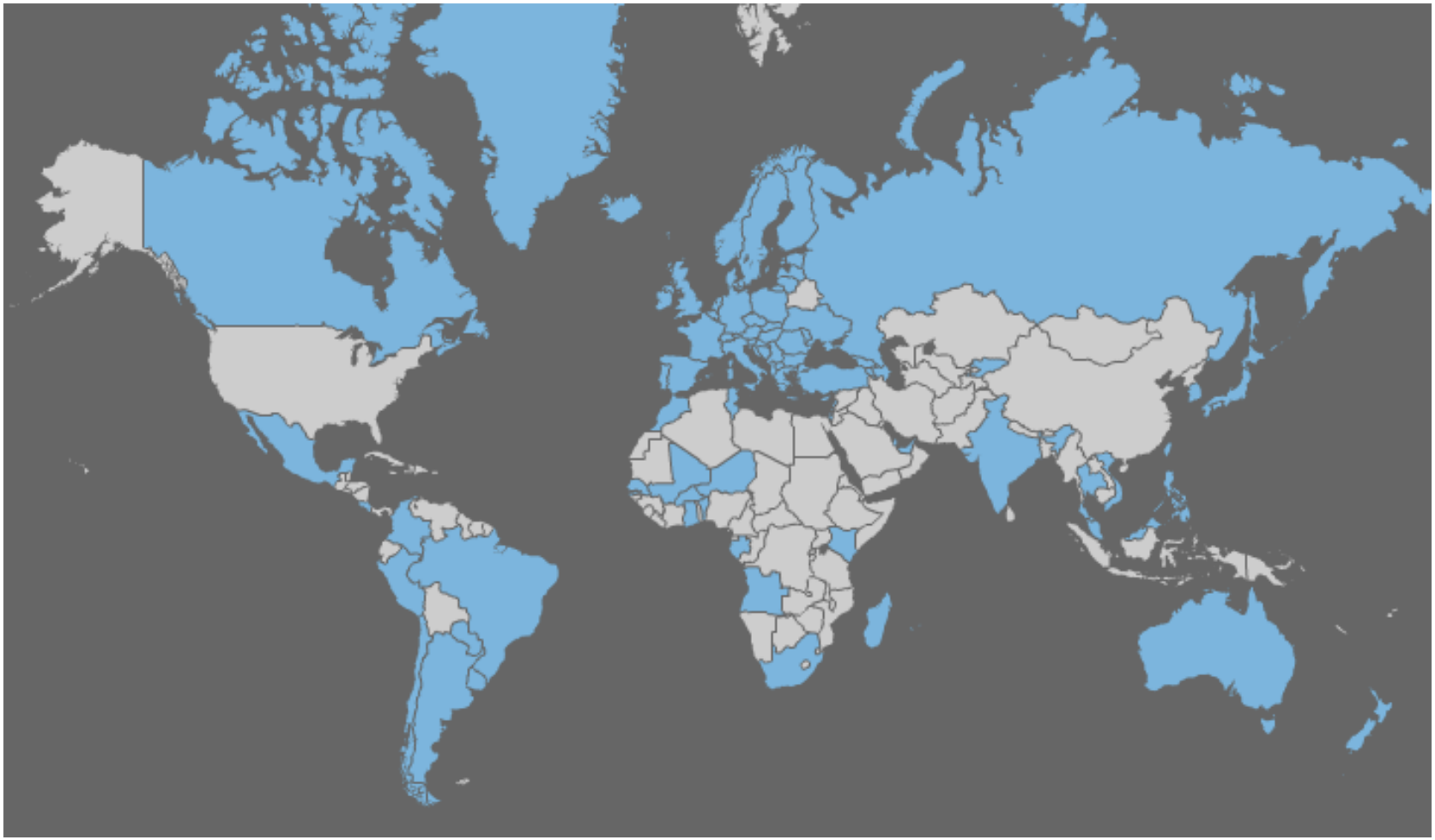
94 jurisdictions with private sector data privacy laws by Nov 2012, with projections to 2020 (linear = 135; accelerated = 160)

Albania • Andorra • Angola • Argentina • Armenia • Australia • Austria • Azerbaijan • Bahamas • Belgium • Benin • Bosnia & Herzegovina • Bulgaria • Burkina Faso • Canada • Cape Verde• Chile • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai IFC • Estonia • Faroe Islands • Finland • France • FYROM (Macedonia) • Gabon • Germany • Ghana • Gibraltar • Greece • Guernsey • Hong Kong SAR• Hungary • Iceland • India • Ireland • Isle of Man • Israel • Italy • Japan • Jersey • Kyrgyz Republic • Latvia • Liechtenstein • Lithuania • Luxembourg • Macao SAR • Malaysia • Malta • Mauritius • Mexico • Moldova • Monaco • Montenegro • Morocco • Netherlands • New Zealand • Nicaragua • Norway • Paraguay • Peru • Philippines • Poland • Portugal • Qatar Financial Centre • Romania • Russia • San Marino • Senegal • Serbia • Seychelles • Singapore • Slovakia • Slovenia • South Korea • Spain • St Lucia • St Vincent & Grenadines • Sweden • Switzerland • Taiwan • Trinidad & Tobago • Tunisia• Ukraine • United Kingdom • Uruguay • Vietnam • ¶

Recent Acts & current Bills

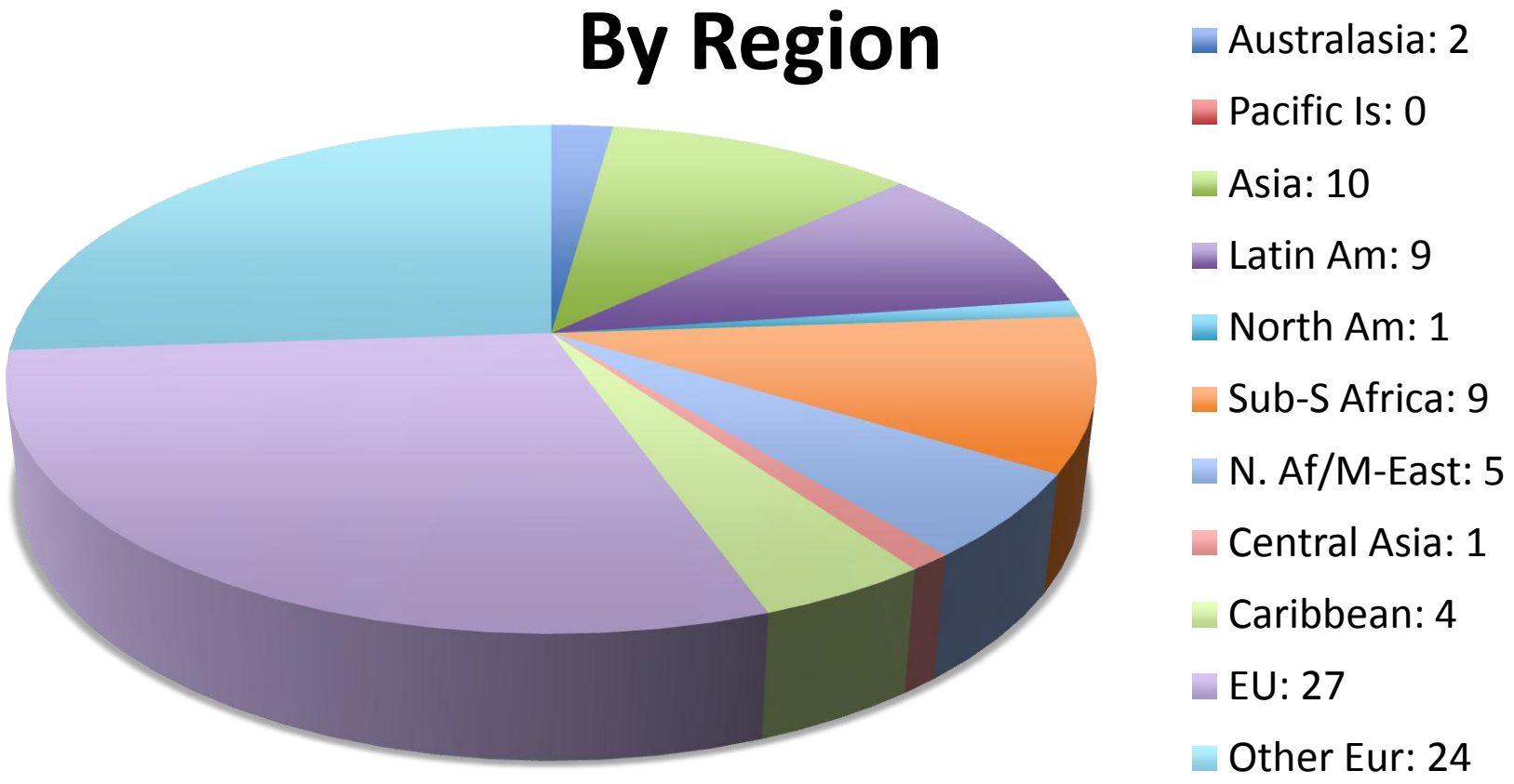
Acts 2011	Acts 2012	Bills pending
Angola	Ghana	South Africa
Costa Rica	Nicaragua	Brasil
Gabon	Philippines	Nigeria
India	Singapore	Kenya
Peru	Yemen	Cayman Islands
St Lucia		+ at least 10 more
Trinidad & Tobago		
Ukraine		
V2.0 of Korea etc	V2. 0 of Hong Kong, Colombia etc	

100+ data privacy laws by 2013 (private sector)



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

Regional spread of data privacy laws



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

A global data privacy map

EU 27	CoE 24
ROW 43	USA 1

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

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

Consequences of globalisation

- Saturation of data privacy laws in countries of economic/political significance by 2020
  - USA and China the only likely outliers
- European laws (EU&CoE) soon in a minority
  - EU laws are only 30% at present, and falling
- ROW cannot be ignored as inconsequential
  - Google: Korea (TOS) and Macau (Streetview)
  - ROW laws keep getting stronger

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’ (next slide)
4. Examined 33/37 non-European laws (as at Dec. 2011) against these 10 criteria
5. Now 43 laws (not 33) but no significant change

10 'European' standards
EU Directive & CoE 108+Add. Protocol
The 2nd Generation Principles

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

An invitation to accede to CoE Convention 108 requires similar

Do non-European laws share Euro-standards?

1. 19/33 countries had *at least* 7 Euro-standards.
2. Average occurrence/law was 7/10 of the criteria
3. 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).
4. New 2012 laws, v2.0 laws & current Bills will not change this – often getting stronger
5. ***Conclusion:*** *Europe's most important standards are now global standards*

10 data privacy laws in Asia

10 Asian data privacy laws

Dated from privacy sector coverage

1. Pre-1995 public sector
2. Hong Kong (1995)
3. Taiwan (1995)
4. S.Korea (2001)
5. Japan (2003)
6. Macau (2006)
7. Malaysia (2009)
8. *Taiwan #2 (2010)*
9. Vietnam consumer (2010)
10. India's 'Rules' (2011)

11. S.Korea #2 (2011)

12. Hong Kong #2 (2012)

13. Philippines (2012)
14. Singapore (2012)

- *Revisions (#2) in Taiwan, Korea and Hong Kong = much stronger laws*
- + Bill in Thailand
- Probably coming in Brunei, Lao PDR, Vietnam #2, Indonesia, India #2

Comparison of 10 Asian jurisdictions *(8 of which are in APEC)*

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. Asian V.2 laws (Korea, HK, Taiwan) much stronger
   - Thai Bill approved by Cabinet will strengthen further;
   - probable Indian v2.0 Act will also be much stronger
4. Ten additional non-OECD principles are shared by at least 3/10 Acts in Asia

Result: Asian laws – despite APEC - are just as 'European' as elsewhere, and growing stronger

Influence of ‘European standards’?

EU 27 99%	CoE 24 90%?
ROW 43 70%	USA 1 20%?

The 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 (v.strong), and may be adopted in Australia and New Zealand; Canada's provision pre-dates APEC

APEC principles have had minimal effect

- CBPRs *might* have some effect (unknown)
- ASEAN may have more effect than APEC

Why have European principles been so persuasive?

Theorists have complementary explanations

- Zaki Laidi (2008) 'Norms over Force'
  - Europe *must* seek influence through norms, because (i) it is not a state; and (ii) norms allow states to share sovereignty without abolishing it.
- Paul Schwartz (2012), citing Bradford's 'Brussels Effect'
  - Bradford finds EU 'trump standards' where non-EU *companies* voluntarily adopt EU standards (like the Directive) because of (i) EU market power; (ii) EU regulatory capacity; and (iii) 'non-divisibility of standards' (difficulty of geographically different standards). Result is adoption of the highest standard.
- There is also a 'Brussels Effect' in the behaviour of States
  - Data privacy laws, overall, evidence a 'race to the top'
  - Reasons are complex, including trade objectives and emulation of a perceived 'global best practice'

Nothing conclusive here – more research is needed

‘Interoperability’
Offer #1: CoE Convention 108

1. Convention 108 + Additional Protocol = Directive (approx.)
2. 43/47 CoE member states have ratified Conv 108
   - 31 have also ratified Additional Protocol
3. Since 2008 CoE has promoted A23 global accession mechanism
   - Uruguay is the first non-European state to accede
   - Standards for accession are similar to EU adequacy
4. Advantage: multilateral free flow of data
   - A consensual bargain, not a unilateral imposition
   - Guarantees free flow not only with UE but with ROW
   - Is a short-cut to EU adequacy as well

But will CoE 108 accession take off globally? Unknown.

Proposed EU Regulation

- 'Regulation' = same rules in all EU states
  - Proposed 2012, probably won't be completed until 2014
- 'Lead DPA' in state of a company HQ
- EU Data Protection Board (= A29 WP)
- Fines for breaches will = 0.5-2% of a company's 'annual worldwide turnover'
- Includes a '3rd Generation' of Principles
  - See list of 14 contenders (over)
- Conclusion: EU is *not* reducing standards
- *Search:* Kuner copernican revolution ssrn

3rd Generation Principles?

From the proposed EU Regulation

1. Explicit consent (opt-in) & proven
2. Explicit data minimisation at collection
3. 'Right to be forgotten', & 3rd Ps informed
4. Right to data portability (copy + format)
5. Regulation of automated 'profiling'
6. Demonstrable implementation
7. Implementation 'by design'
8. Implementation 'by default'

3rd Generation Principles? (cont)

9. Liability of processor local representative

10. Data breach notification

11. Privacy Impact Assessments required

12. Data Protection Officers required

13. Data exports require (i) 'adequacy' OR (ii) BCRs OR (iii) DPA approval

- CoE 108 compliance may assist adequacy

14. EU rules apply to extra-territorial offering of goods/services or monitoring

‘Interoperability’: Offer #2: US ‘Consumer Privacy Bill of Rights’

- CPBR = Obama Administration 2012 initiative
- From a US perspective, it’s a valuable initiative
  - The 113th Congress does not seem likely to increase regulation of the whole private sector
  - US privacy advocates have to work with the possible

What does the CPBR offer of value to Europe and the ROW?

1. CBPR does not fully meet the OECD Guidelines (particularly 'finality' principles) – '*inadequate*'
2. OECD may no longer be an attractive deal, particularly in light of the proposed Regulation
3. Is CPBR achievement *realistic*?: does not justify 'interoperability' until delivery demonstrated
4. 'Known unknown': can the US *ever* protect 'finality', in light of constitutional issues?
5. APEC's Cross-Border Privacy Rules (CBPR) are an *unlikely* basis: based on 'OECD lite'; methods of enforcement may be too weak; cumbersome

Where does this leave the US' privacy relationship with everyone else?

- Full 'interoperability' with US standards is will be premature for a long while, 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. Inevitable administrative inconvenience for US companies in complying with BCRs, Safe Harbor etc
  3. More frequent problems for US companies (prosecutions, fines, damages) across the ROW
  4. Voluntary adoption by many US companies of increasingly global 'European' standards

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/ has links to both