PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Asian Data Privacy Laws

MORNING WORKSHOP

5 October 2018, Linklaters, London

Hosted by

Linklaters

Sponsored by

OneTrust
Privacy Management Software

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Asian Data Privacy Laws Workshop

Professor Graham Greenleaf AM

Professor of Law & Information Systems,
University of New South Wales

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

Linklaters, London, 5 October 2018

Relevant materials

1. Greenleaf ***Asian Data Privacy Laws*** (OUP, 2014) – Comprehensive text on all 26 Asian jurisdictions, to early 2014 – available in paperback.

2.2014-17 Update to ADPL (to 07/17) Online on SSRN

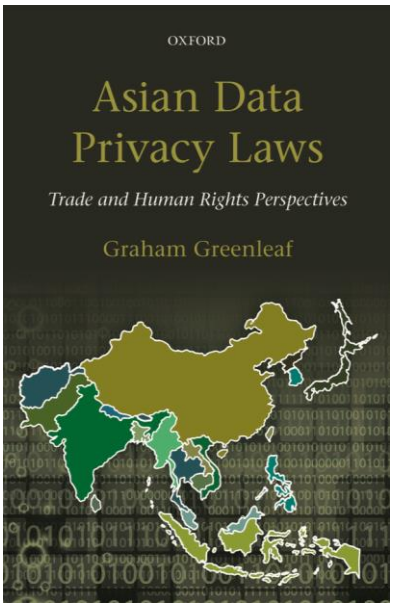
1. **2017-18 Further Update** to ADPL (to 10/17) Available online later in 2018.

2. **New online**: Twitter @grahamgreenleaf

1. Articles in ***Privacy Laws & Business International Report***

2.ABLI *Regulation of Cross Border Transfers of Person Data in Asia*, 2018

1. International Privacy Law Library …



2

International Privacy Law Library on WorldLII

<http://www.worldlii.org/int/special/privacy/>

– free extensive online resources

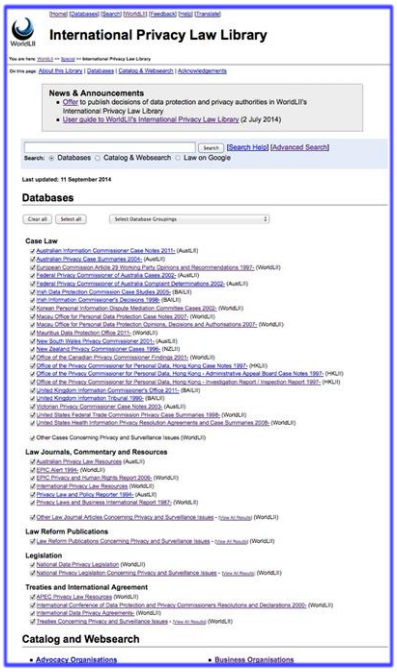
– includes **all Asian Acts discussed**, in English, in National Data Privacy Laws database

– all **international agreements**

– includes **cases decided** by these DPAs (and others):

- Hong Kong PCPD
- Korean PIDMC
- Macau OPDP

– many **journal articles** etc

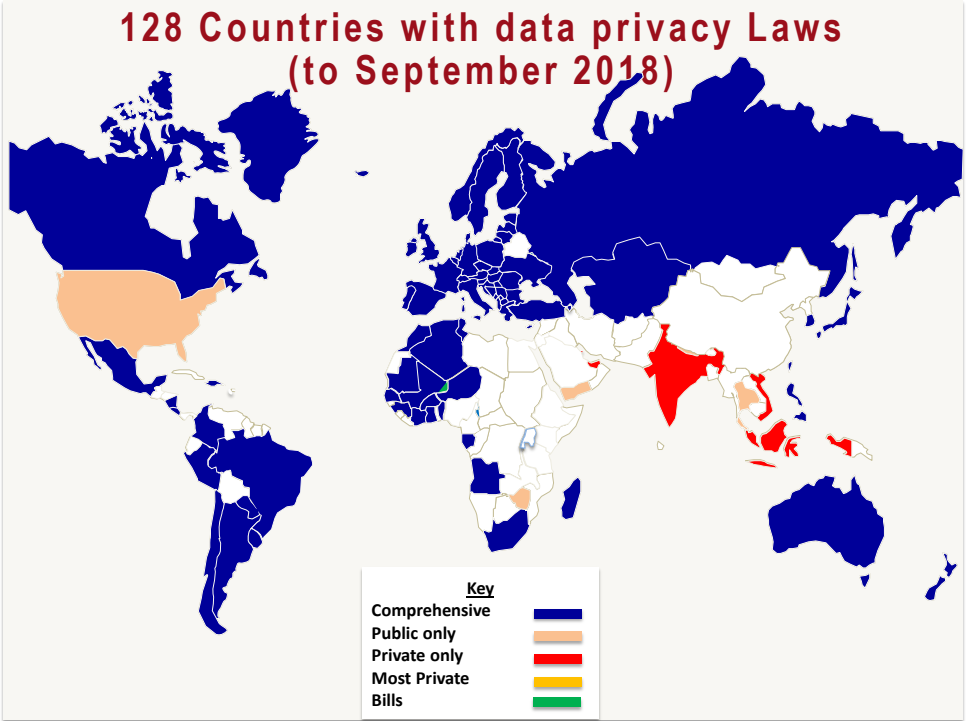


3

Global Context: How many countries now have a data privacy law?

- Answer: **128** (as at September 2018)
  - 2017 Tables and articles on my web pages/SSRN: 120
  - Since then, Cayman Islands, Mauritania, Niger, Guinea (Conarky), Brazil, Algeria, St. Kitts & Nevis, & Bahrain
  - Since 2014 the majority of global privacy laws are from **outside Europe** (now 75/128)
- 90% have a **separate Data Protection Authority** (DPA)

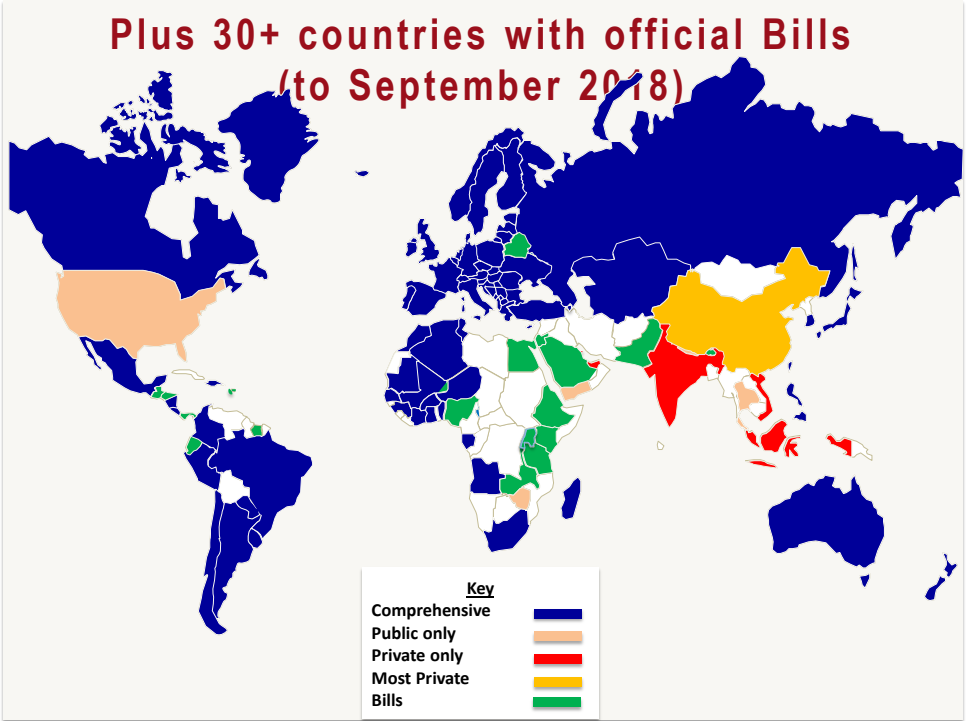
4



5

What principles do the 128 laws enact?

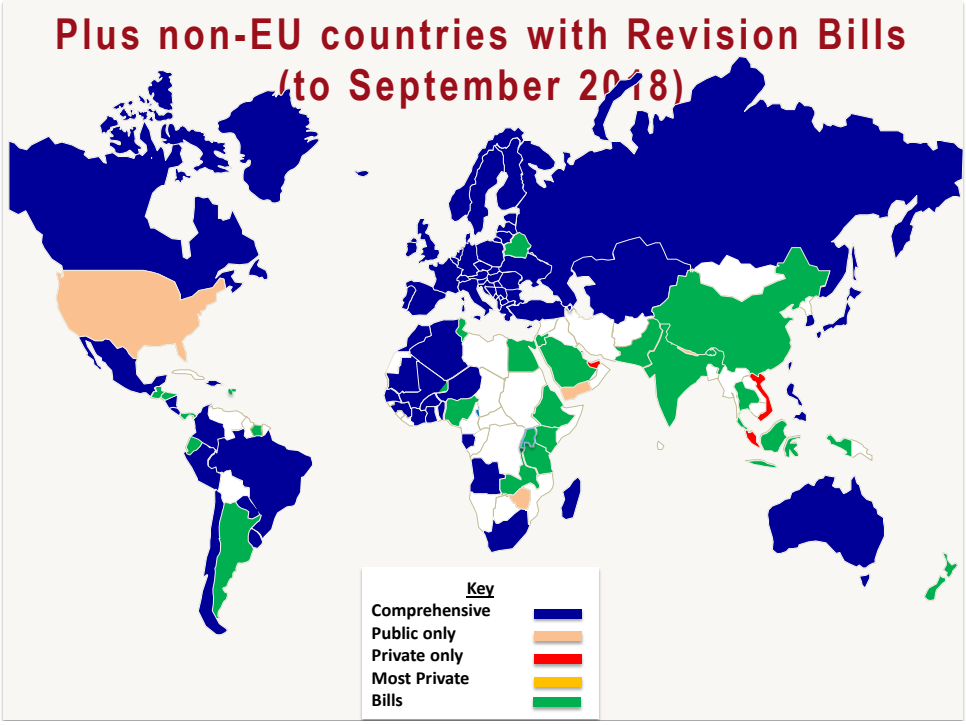
- 1980s: OECD Guidelines & CoE Convention 108 had 9 common elements which defined a 'data privacy law'
- The 1995 EU Directive contained **10 principles** not found in the 1980s standards – a '2nd generation'
- The current 128 laws include, on average, at least 7/10 of these '2nd generation''principles
- The 'Top 20 by GDP' countries outside Europe with a law include on average 6/10 (2017)
- Therefore, **the current 'global standard'** is at least half-way to the Directive's standards
- From 2018, GDPR-influenced laws around the globe are rapidly **raising this standard**



7

Bills for new & revised laws

- About 30 more countries currently have **official Bills**
- Growth of new laws globally has **not slowed down**
  - Annual average of 2.4 countries with new laws since 1970
  - This decade, the annual average is **5 new laws**
- Many stronger "2nd generation" **revised** laws
  - Many **already enacted**, for example in Asia-Pacific: Korea, Hong Kong, Taiwan, Japan, Australia
  - Now many **post-GDPR revision Bills**: Tunisia; India; Argentina; Indonesia; Thailand; New Zealand
- Some significant e-commerce/consumer privacy laws
  - eg China's laws may soon become a full data privacy law



9

Early effects of the GDPR

Survey of **over 30 countries outside Europe**, shows these 'GDPR principles' enacted by **at least 10 countries**:

- *DPAs enabled to make binding decisions and issue administrative sanctions including fines;*
- *Right to object to processing based on controller or public interests;*
- *Data breach notification to DPA & to data subjects (+ US);*
- *Stronger consent requirements;*
- *'Sensitive data' to include biometrics and/or genetic data;*
- *Mandatory Data Protection Officers (DPOs) for some processing.*

All other new GDPR principles were adopted by 1-9 countries

11

Far away – Asia's 26 jurisdictions

Regional vs National Structures

Regional Structures	Europe	Asia
	56 countries and territories	24 countries + 2 SARs
Regional Legislatures	EU and CoE	None
Permanent bureaucracies	Brussels & Strasbourg	None (not ASEAN, nor APEC, nor SAARC)
Common privacy rights	EU Charter; Directives; GDPR; ECHR A8; Conv 108/108+	None (only 5/26 accept ICCPR Optional Protocol)
Regional courts	ECtHR; ECJ/CJEU	None
Regional DPA groupings with functions/powers	Article 29 Working Party; EU Data Protection Board	APPA is informal; APEC CBPR JOP approves proposals

13

14/26 Asian countries with data privacy laws (or close to…)

1. Japan 1988 (public sector) + private sector 2003
2. South Korea 1995 (public sector) + private sector 2001
3. Hong Kong 1995 (comprehensive)
4. Taiwan 1995 (public sector + limited private sector)
5. Thailand 1997 (public sector) Comprehensive Bill 2018
6. Macau 2006 (comprehensive)
7. Nepal 2007 (public sector)
8. Malaysia 2009 (private sector)
9. Vietnam 2010 (private sector)
10. India 2011 (private sector) Draft comprehensive Bill 2018
11. Philippines 2012 (comprehensive)
12. Singapore 2012 (private sector)
13. Indonesia 2012 + Regulation 2016 (private sector) Comprehensive Bill 2018
14. *China 2011-18 (most private sector) But no access right*

+ Bills in (15) Pakistan, (16) Bhutan

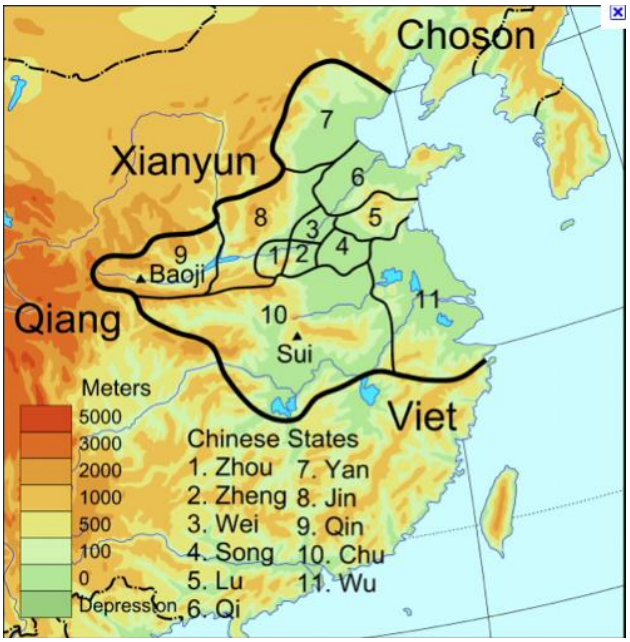
Revised laws

15. Taiwan 2011(comprehensive)
16. South Korea 2012+++
17. Hong Kong 2012
18. Japan 2015

Asia overview

1. The GDPR has caught on
2. Different countries are at different levels of maturity
3. There is convergence and divergence
4. Enforcement?

China



Map of China in the 'Warring States' period

17

China – The overall picture

[ADPL Ch 7 'From Warring States to Convergence']

- *Context* – A one-party state relying on intensifying pervasive surveillance and censorship.
  - State interests will always override privacy.
  - Otherwise, consumer privacy is being given a surprising degree of respect and protection – at least for some people
- The sources of privacy protection are extremely complex, and still not comprehensive, even in the private sector.
- The key points are to understand (i) their scope; (ii) the interaction of protections; and (ii) the extent of their consistency.

18

China – The overall picture (2)

New 'cyber-sovereignty' ideology of Xi Jinping regime

- See work of Rogier Creemers, Scott Livingston, Anne Cheung etc

– Internet as a central(ised) means of governing society and party:
  - new Central Leading Group for Cybersecurity and Informatization (Chair: Xi Jinping),
  - enhanced role of Cyberspace Administration of China (CAC)

– Increasingly 'securitised' and seen as a threat:
  - technical security (post-Snowden), affecting banking software etc;
  - ideological security (greater cultural, social media censorship)
  - Social credit system merging public and private data sources
  - More surveillance intensity though CCTV + face recognition

– A distinct Chinese approach to global cyber-governance
  - Since White Paper on Internet (2010), Internet seen as an extension of national sovereignty (eg localisation of health information servers)
  - Rejects multi-stakeholder processes in favour of governments

Result: Post-2012 partial retreat from the rule of law

19

China – Regulation time line

1. 2006/7: Draft *Personal Information Protection Act,* from Institute of Law; private & public sectors; included DPA; EU-influenced
2. Some *Provinces* enacted consumer privacy codes; *Piecemeal* laws on money laundering, medical records, insurance, credit reporting etc
3. 2009-10 Major reforms: *Criminal Law* and *Tort Liability Law*
4. 2011 MIIT (Min. of Industry & Info. Tech.) 'Internet Information Services Regulations'
5. 2012 NPC Standing Committee 'Decision' (a law) on Internet Information Protection
6. 2013 MIIT Internet/telecommunications Regulations
7. 2013 MIIT Standardization Administration 'Guidelines' on Personal Information Protection in 'computer information systems'
8. 2013 Consumer Law amendments by NPC Standing Committee
9. **2016 Cybersecurity Law – most comprehensive & broadly applicable law yet**
10. **2018 Privacy 'Standard' (not a law but probably treated as such)**

(See Update pp. 18-24 & Further Update p. 5 for these last two)

Result: No comprehensive national law yet; 'Warring States' period 2006-10; consistent direction emerging 2011-13; increasing cyber-security emphasis since then.

20

China – Emerging principles in 7 laws & standards, 2011-18

1. Either (i) a general 'fair processing' principles (in 3); or a detailed set of basic privacy rights (***except*** for access rights).
2. *'Personal information'*: based on capacity to identify (ie conventional) – 2018 Standard has broadest definition
   - 'Sensitive' data generally not distinguished until 2018 Standard
   - De-identified data only exempted if identity 'cannot be recovered'
3. *Collection:* consistently limited to what is necessary for purpose ('minimal collection')
   - Only MIIT Guidelines limit unfair methods of collection
4. *Notifications* at time of collection required
5. *Limits on use / disclosure:* Uncertain: CyberSec law more clearly limit these to purposes of collection (NPC-SC laws do not).
6. *Data quality: still* generally vague on data integrity etc

21

China – Emerging principles (2)

7. *Security:* general requirements only
   - But data breach notifications to authorities is always required (to data subject only in one)
8. *Accountable controller* always required
   - Public privacy policy required by 2/5
9. *User rights* are a weakness
   - Correction explicit in CyberSec Law, impled earlier;
   - Access not explicit in CyberSec Law, only in 2018 Standard
10. *Data export limitations* only explicit since Cybersec Law (over)
11. *Direct marketing:* Both NPC-SC laws require consent
12. Restrictions on automated processing – in CyberSec Law

Conclusion*:* An emerging set of consistent principles, now stronger than OECD Guidelines (except access), but diverging widely on data localisaiton exports and export

22

China – Cybersecurity, data localisation, & export restrictions

- *Update* pp 21-23; *Cybersecurity law* (2016); *draft Security Measures* (2017) (not finalised); *Draft Regulations on …Cybersecurity* (June 2018)
- Key Information Infrastructure Operators (KIIOs) defined
  - obligations re personal & 'important' data (KII data)
- Two forms of data localisation (attacked in WTO by US/EU)
  1. KII data requires *storage* in 'mainland China' (localisation #1)
  2. Export of some data is *prohibited* (localisation #2)
- Other KII data can be *exported* only if
  1. export is 'truly necessary' to business; &
  2. security review passed (some can be self-assessment) &
  3. Data subject consent obtained, after detailed notice.

China – Enforcement of laws & standards

1. No DPA, complex Ministry-based enforcement, under overall guidance of the Cyberspace Administration of China (CAC), by
   - Ministry of Industry & Information Technology (MIIT)
   - State Administration of Industry & Commerce (SAIC)
   - 'Telecommunications authorities' at all levels
2. **Administrative orders**, penalties & publicity: 6 types are provided (fairly consistently) by these laws
   1. Issuing warnings
   2. Orders for rectification / cessation of processing
   3. Administrative fines
   4. Confiscation of profits/illegal earnings, + punitive fines
   5. Adverse publicity, including in the press, and reports to MIIT
   6 Employment prohibitions; suspension/termination of businesses
3. **Civil damages** – Consumer right of court action, often on the same basis as administrative fines (+ emerging actions under the Tort Law and the revised General Provisions of the Civil Law 2017)
4. **Criminal offences** – Generally proceed under the Criminal Law

24

China - Criminal Law

- A 253 Criminal Law (7th Amendment, 2009)
  - Criminal penalties for institution or employee selling, otherwise illegally disposing, or offering to sell personal information if 'serious'
  - Covers employees of government, hospitals, schools, and telecomm, financial, or transportation companies (+ 'etc')
  - Penalties also apply to those 'illegally obtaining' such data
  - Sentence up to 3 years plus monetary penalties
  - Reinforced by cl 1 of 2012 NPC Standing Committee 'Decision'
- Enforcement of A 253
  - There have now been at least 260 prosecutions; some examples:
  - *Wang Shengrong case* (2009): identity theft case to allow daughter to obtain educational credentials of victim (facts like *Qi Yuling* case)
  - *Zhou Jianping case* (2010): illegal purchase of log of telephone calls by high government officials; sold to others who used it logs to fraudulently impersonate officials. Purchaser sentenced to 18 months, others prosecuted for fraud.

(continued over)

25

China – Criminal law (2)

- Art. 253A (cont)
  - *Shanghai Roadway case* (2012): jail sentences of up to 2 years for four former executives of D&B's China subsidiary, for purchasing data on 150M Chinese customers of insurance companies, banks.
  - *Humphrey case* (2013): Update p. 19 – UK expat Humphrey and his US citizen wife ran a business intelligence service ('ChinaWhys') in Shanghai. Convicted of illegal obtainment of 256 files of personal data, at about US$200 per file. Given 2.5/2 year jail sentences and US$56K fine. Did not matter that sellers were not from the listed industries ('etc' may mean 'service industries'). What is 'serious'?: here, files were less numerous than other cases, but may have interfered in a corruption investigation [Livingston & Greenleaf]
- Conclusion: A 253A is likely continue to be a significant enforcement aspect of more serious privacy breaches in China
  - Foreigners are clearly not immune to this aspect of Chinese law

26

China – Tort law

- Constitutional right to privacy cannot found civil cases
  - Supreme People's Court 2008 declaration that its *Qi Yuling* decision (2001) (on ID theft and the right to an education) no longer applied.
- *General Principles of Civil Law* (CPCL) 2017
  - Little progress under previous version – Privacy issues treated as defamation cases, following Judicial Interpretation (SPC) holding privacy to be subsidiary to the right of reputation - some succeeded.
  - Example – *Wang Fei Case* (2008): Website operator held liable for defamation, for website about the husband of a woman who committed suicide, resulting in him being harassed. Apology and compensation of about $1,000. (Appeal decision in 'human flesh search engine' case). Importance of case continues in the factors it sets out as to what constitutes an infringement of privacy.
  - 2017 new GPCL: 'right to privacy is now a specific individual right (**Update** p. 23)
- *Tort Liability Law* 2009 - **Update** pp. 19-20
  - A 'right to privacy' (undefined) is included in the list of 'civil rights and interests', the breach of which leads to civil liability
  - Employers are vicariously responsible; ISPs are liable for torts committed using their networks, unless they take sufficient steps after notice (A 36)

27

China – Tort law (2)

- *Supreme People's Court Regulations* (2014) **Update** p. 20
  - 'Concerning .. Handling civil dispute cases involving the use of information networks to harm personal rights and interests'
  - Only deals with privacy interferences via networks (A 36 of TLL), not 'off line' interferences.
  - Comprehensive 19 Article direction to all Chinese courts on handling cases under GPCL, TLL and NPC-SC Decision
  - Deals with substantive as well as procedural issues
  - Covers jurisdiction, joinder of parties, procedure, standards courts will apply on key questions of fact, sensitive information, remedies (apologies, damages etc)
  - Its application will affect all future cases of 'privacy torts via networks', and make such cases much more likely to arise.
  - Some minor cases, mainly to resolve disputes between individuals, and not commercial matters – but new cases under SPC Reg are not known.
- **Result**: GPCL, Tort Law, & SPC regs provide a legislative civil action that *Qi Yuling's Case* ultimately failed to constitutionalise, but as yet civil actions are not a major feature of Chinese privacy law.

28

China – the cybersecurity law one year on

1. A data protection law by any other name
2. Can I take my data out of China…..or not?
3. Conflating security and data protection
4. Who's my regulator?

[ADPL Ch 8 'Japan – The Illusion of Protection']

Japan

- Privacy rights outside PPIA
  - Implied constitutional protection of privacy under A 13; never yet breached!
  - Civil CodeL some negligent disclosure and 'right to forget' cases
- Complexity of the main legislative structure (2003-)
  - *Protection of Personal Information Act 2003* (PPIA) covers both private sector (principles and enforcement) & public sector (principles only)
    - 4 other Acts cover enforcement in the public sector etc
  - The *'Basic Policy'* and the *Cabinet Order* on enforcement (both rev 2008) are relevant to all
  - 38 (non-binding) *Guidelines* for the private sector(s) set by each Ministry
    - Rationalisation based on METI Guidelines (rev 2009)
  - 1799 municipal *Ordinances* on data protection
- 2015 PPIA Amendments – see ***Update*** pp 24-25
  - Major changes, closer to international standards
  - Created a DPA (PIPC) for 1st time, with independent status
  - Only in effect since May 2017: no track record yet

32

Japan – Privacy Principles (post-2017)

- **Access and correction** rights are now explicit
- **Deletion** requirement for the first time
- **Disclosure** limitation is **undermined** by ability to merely publish on a website (non-identified) details of intended disclosures and invite opt-outs (A 23(2));
  - Notice also required to PIPC , who must also publish it
- **Collection** is **not explicitly limited** to what is necessary for the specified purpose (A 17)
- **Data export limitations**, with PIPC to decide Whitelist; PIPC can allow exports to APEC CBPRs compliant companies (the 'Japanese back door')
- Some notification of data breaches (**DBN**) required

Result: *Japan's principles were OECD basics or less; now closer to Asian average of 5/10 'European' principles*

33

Japan – (non)Enforcement (pre-2017)

- No basis for damages claims before Courts (or anyone else)
  - No provisions in Act for payment of compensation
  - Breach of PPIA does not give civil damages claim (2007 Tokyo District Court)
  - 2018 *Benesse* decision that birthdates of 35M children was 'not private enough'
- Investigation of complaints under PPIA
  - Complaints may be filed with 4 types of bodies: (i) the business; (ii) 39 APIPOs (sectoral business bodies); (iii) local government; or (iv) National Consumer Affairs Centre – BUT not the relevant Ministry (which has enforcement power). But PPIA sets out no procedures.
  - Only published outcomes are for 13 complaints to the National Consumer Affairs body from 2004-07: they explain nothing
  - No evidence of any outcomes by other mediation
  - The complaints system has zero transparency
- Enforcement by Ministries
  - Ministries cannot issue fines; they can collect reports (often); make recommendations (7 in 7 years); and issue compliance orders (ø in 7 years) – so there are ø prosecutions for non-compliance.

Bottom line = no evidence of enforcement

34

Japan – Enforcement? (post-2017)

- Previous 'Ministry-based' system replaced by PIPC as a DPA for the private sector
  - Ministry of Internal Affairs (MIC) for public sector
- PIPC (9 Commissioners) has strong legal independence
- PIPC Rules will implement Act & Cabinet Order
- PIPC has strong powers to investigate, find breaches, and give advice/recommendations/orders
- No PIPC administrative penalty (except US$3K for disobeying PIPC orders) or compensation powers
- Fines following prosecution are trivial (US $10K)

Q: Will PIPC use powers any more than Ministries didn't?

Japan – Legalising 'Big Data'

- 'Anonymous processed information' (API) – PPIA requires PIPC to specify de-ID procedures which may be impossible – uncertainties
  - But API status results from following procedures, not from achieving making re-identification impossible
- Bulk API then becomes able to be disclosed/sold to others, but both discloser and recipient still have significant security and publicity obligations
- Will there be a business case for use of API?

Japan – EU adequacy status

- See Further Update pp. 6-7
- EU Commission draft Decision = 'adequate'
  - But other EU bodies can influence final result: EDPS; EDPB; LIBE Committee; Committee of States; subsequently NOYB (Schrems) etc ; CJEU
  - Correct decision is vital to credibility of adequacy; other countries will say 'I'll have what Japan had'
- Japan's PIPC will issue 'Supplementary Rules' **applying *only* to EU-sourced data**:
  1. Additional 'special categories' (sensitive data).
  2. Preservation of protections with no time limits.
  3. Preventing adding disclosures simply by website notice
  4. Requiring that API be 'irreversible for anyone' (ie objective)
  5. Onward transfers to US companies based solely on APEC-CBPRs certification is blocked – replaced with a consent requirement

Japan – EU adequacy status (2)

- Issues raised in my articles not yet addressed, or still unclear:
  1. Transparency – including reliability of translations
  2. Are the Supplementary Rules binding?
  3. Applicability to public sector? (no Annexures yet)
  4. Public sector access to private sector data? (*Schrems*) (no Annexures yet)
  5. 'Readily collated' requirement in PI definition: will some EU personal data not be protected?
  6. Still no evidence of enforcement; How is Japan's enforcement regime 'essentially equivalent' to EU?
  7. Is consent a sufficient basis for an onward transfer regime?
  8. Can an 'essentially equivalent' law exclude Japanese citizens?
- Other gaps between Japan and EU:
  - automated decisions; design & default; DBN; data portability
  - How important are these to adequacy? ('essentially equivalent')
- Bottom line = It isn't over until it's over

[ADPL Ch 5 'South Korea – The Most Innovative Law']

South Korea

- *Context:* Since 1980s, one of world's most successful transitions from dictatorship to democracy – very strong democratic and civil libertarian elements. Also the most Internet-intensive country.
- Strong *constitutional protections* via Constitutional Court
- Civil Act gives *tortious action*, used in mass data breaches
- Three largely consistent *data privacy Acts*:
  - Comprehensive *Personal Information Protection Act (PIPA) (2011)* added many new features including 1st DPA (PIPC)
  - BUT 'Network Act' (under Korean Communications Comm) continues to govern ISPs & ICSPs – see ***Update*** p 15.
  - Similar sectoral Act governs finance industry.
- Result has become an intense 'turf war' between agencies
- Continuous strengthening of all enforcement since 2011

Overall assessment: Strongest data privacy laws in Asia

40

South Korea – Additional principles

PIPA 2011 includes **all basic OECD principles**, plus **these additions**:

1. **Onus** of proof of almost all requirements is on the processor
2. Privacy Policy necessary, and overrides any individual agreements where this favours the consumer (A 30) (strong **transparency**)
3. **Minimal** collection of personal data necessary for purpose (A 16(1)
   - Desirability of 'anonymity, if possible' of processing (A 3(7))
4. No denial of services because of refusal to provide unnecessary information (A 16(2)) + 2013 amendment requiring notice of this (**unbundling** consents)
5. Sensitive data cannot be processed without consent (A 23)
6. Alternatives to identification by the Residence Registration Number must be provided (A 24) [RRN use is separately being prohibited]
7. Strict limits on operation of visual surveillance devices (A 25)
8. **Notification** required if personal data collected from 3rd Ps (A 20)
9. Consent required to disclose to 3rd Ps, who must be identified (A 17)
   - limited exceptions (A 18) *not* including 'compatible uses'

41

South Korea – Additional principles (2)

10. Data exports require consent (A 17(3)) - but notice is weak
11. **Notice of sub-processing** is required (A26), and must be identified
    - OR public Privacy Policy (PP) can give notice of sub-processing
    - sub-processors are deemed employees (A 26(6)) (vicarious liability)
12. **Deletion** (not de-ID) of personal data required after use (A 21)
13. **Suspension** of processing can be required by data subject (A 37)
14. **Privacy Officer** must be appointed, with detailed duties (A 31)
    - MOSPA Guidelines do not specify any size limit of business
15. **Data breach notification** always mandatory to data subjects (A34)
    - Also to MOPAS and other authorities if 'large scale'
    - 'Surcharges' of up to $0.5M if RRNs are negligently lost
16. Offences to improperly deal with, disclose or receive personal data
17. Detailed security measures are prescribed by Presidential Decree, both locally and for data exports

These 17 points mean Korea does cover ***most*** elements of the GDPR

42

South Korea – Range of enforcement measures (1)

- *Compliance orders/ admin fines (see Update, pp 15-170)*
  - Ministry and other agencies can issue compliance orders and administrative fines (468 in 2013).
  - 'Administrative surcharges' (fines) of up to 3% of business turnover; as yet, one US$4.5M surcharge by KCC on a shopping mall for negligence
- *Criminal offences*
  - Complex lists of which breaches attract which penalties
- Data subjects may *sue for damages for breach* (A 39)
  - Onus of proof of no intent/ negligence is on data user
  - Many actions, including class actions: Held that massive data leak did not automatically result in damages for mental distress (2011)
  - Reforms**: Statutory damages** (no proof of actual damage) of US$3K/head for data breaches (some have 1M+ claimants);
  - **Punitive damages** = treble actual damage

43

South Korea – Enforcement (2)

- *Collective dispute mediation* by PIDMC (A 49)
  - Where multiple data subjects are affected, any parties can request PIDMC to undertake collective dispute mediation
  - Presidential Decree sets out procedural details. Mediation continues even if some complainants go to Court
- *Class actions* (Part 7 'Data protection collective suit')
  - If processor rejects collective mediation, various types of NGOs (defined in Act) are entitel to file a class action ('collective suit')
  - Suit is filed in the District Court of the defendant's place of business, or main office of foreign business's representative (A 52)
- *Self/Co-regulation is not significant*
  - No provisions concerning enforceable codes in new Act
  - MOPAS is required to facilitate self-regulation
- **Adequacy issue – independent powers**
  - PIPC is not independent from Ministry in its exercise of powers
  - KCC is independent, and with even stronger powers: result may be a sectoral assessment for online ISPCs regulated by KCC

44

Korea – **Issues for EU adequacy**

- ***Update*** pp 12-18; 2018 adequacy article; ***Further Update*** pp 8-9
- Korea applied for adequacy 2016; being assessed after Japan
  - only applying in relation to ICSPs under its Network Act; KCC is DPA

1. Defn of 'personal information' (PI) in PIPA & Network Act
   - only applies where '*easily* combined' to enable identification (some English translations)
   - KCC and other agencies relied on this to 'carve out' such data as not PI
   - but *IMEI decision* (Seoul District Court, 2013) interpreted PI very broadly to include any possibility of obtaining data, even if a court order was necessary to do so.
2. Big Data/ de-identification Guidelines (2016)
   - If data is PI, de-ID procedures specified, and security etc rules still apply
   - 2018: Korean agencies agreed to **adopt EU definition** of anonymous data so as to strengthen adequacy prospects

Result: Both definition of PI & of anonymisation, are consistent with GDPR

Korea – **Issues for EU adequacy (2)**

3. Data export and onward transfer restrictions
   - Network Act art. 63 allows data exports based on consent:
     - specific notice requirements (destination country and company, purpose, retention period, security)
     - Up to 3% turnover fines for exports without consent
   - Amendts to Network Act 30/8/18 (Further Update p. 9):
     - Purports to bind overseas recipient similarly (cl 63(8))
     - Gives KCC power to suspend any cross-border transfers if risk of severe violations of users' rights (cl 63(5))
     - Foreign businesses must appoint **local agent**; joint liability
4. Who will benefit from changes?
   - Everyone (contrast Japan)

Case Study 1 – using centralised HQ functions

Case Study 1

1. Consent v notification for processing
2. Cross-border transfer requirements
3. Are any other laws applicable?

Case Study 2 – M&A deals

Company A

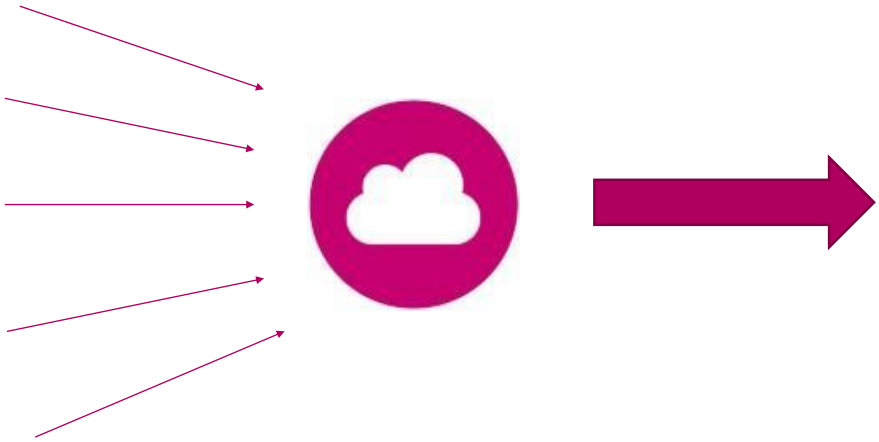
↓

Company B

Case Study 2

1. Sufficiency of consents or notices
2. Refreshing consents
3. Access controls
4. Any breach issues?

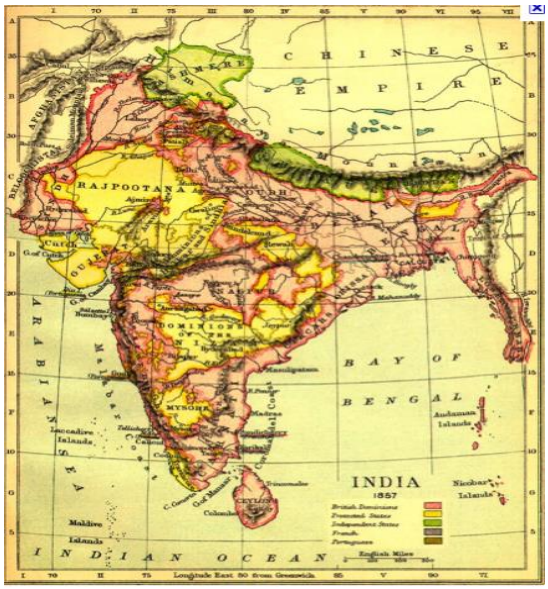
Case Study 3 – big data and digitisation



Case Study 3

1. Processing grounds; cross border transfer
2. Anonymisation
3. Local law quirks (e.g., data matching under PDPO)
4. Ethical issues

India



India in 1857 – 'The Great Rebellion'

53

India – Overview

[ADPL Ch 15 'India – Confusion Raj, with outsourcing']; ***Update***, pp33-36

- *Context:* World's largest democracy, with often-functioning rule of law, despite consistent problems of corruption. Huge outsourcing.
- India's legislative privacy protections are piecemeal; its supposedly general 'Rules' of 2011 are in fact very limited and useless
- India twice failed to obtain a adequacy finding from the EU (most recent 2013)
- Crucial question: Does the Indian Constitution imply a privacy right?
  - A 21 protection of 'personal liberty' is the basis
  - Was mainly used to limit search and surveillance'.*Naz Foundation Case* (2009) extended previous case by holding unconstitutional legislation criminalising homosexuality, based on autonomy; but SC appeal (2013) overturned this. ; Supreme Court had not expanded this right to 'informational self-determination
  - The Aadhaar ID number system was attacked as being unconstitutional, with Mr Puttaswamy (92 year old SC judge) as one of the petitioners…

54

India - *Puttaswamy*'s consequences

Further Supplement pp. 15-21

- In *Puttaswamy v Union of India* (2017) the Indian government argued there was no constitutional right of privacy at all; in August 2017 a nine judge 'constitution bench' of the Supreme Court found there was an inalienable fundamental rights of privacy
  - three main aspects of privacy: privacy of the body; privacy of information; and privacy of choice.
  - Any legislation/government actions affecting privacy must be (i) for legitimate state interests; (ii) necessary and proportionate; & (iii) authorised by law.
- All Indian privacy issues are now in flux in light of *Puttaswamy:*
  - *Navtej Johar v Union of India* (6 September 2018) – five judge Constitution Bench held criminalisation of homosexual conduct was unconstitutional (reversing result of 2013 *Naz* appeal).
  - *Puttaswamy #2* – Challenge to constitutionality of Aadhaar biometric ID system to be decided by 5 judge Constitution Bench by 30/09/18.

India – Srikrishna Report and draft Personal Data Protection Bill 2018

- *Modi government's imperatives*:
  - To save the Aadhaar (depending on *Puttaswamy #2*) and many other government schemes, it will need to show that the invasions of privacy involved are 'necessary and proportionate' through legislation that *sufficiently* protects privacy against abuses.
  - To obtain a positive adequacy assessment from the EU, particularly to benefit its outsourcing industry
- Srikrishna Report (July 2018) recommended draft *Personal Data Protection Bill 2018*
- Indian government (DeitY) has now called for submissions by 30 September
  - It is between a rock and a hard place

India – draft Personal Data Protection Bill 2018 (2)

- See Further Update pp. 17-18 for key features of the draft Bill, compared with GDPR
  - Many key features are included, but with more prescriptive approach than the EU's decentralisation of responsibility/liability to controllers
  - GDPR elements excluded may not be important
  - Potentially very strong enforcement by a national DPA, including up to 4% administrative fines
  - Combined with strong data localisation requirements (Chinese influenced?) and data export limitations

India's new data protection bill

1. Extra-territorial application
2. Data localisation and cross-border transfer
3. Consent, consent, consent
4. Breach notification
5. Some controllers are more equal than others
6. Penalties

Expected Asian Developments 2019

Current key Asian developments

- Region of **most rapid current growth** which will continue in 2019
  - Many new/revised GDPR-influenced laws
  - Changing from 'private sector only' to comprehensive laws
- **Thailand** – comprehensive GDPR-like Bill
  - will go to legislature soon, may be enacted quickly
- **Indonesia** - comprehensive GDPR-like Bill
  - will not be enacted this year, but probably will in 2019
- **China** – current laws likely to have missing right of access added;
  - **data localisation** will continue tensions with US, EU etc
- **India** – draft Bill with strong GDPR influences will be enacted
  - Chinese-influenced **data localisation** will be controversial outside India
  - *Puttaswamy* Cases #1 (constitutional right) will shape final Act
  - *Puttaswamy* Case #2 (Aadhaar) saves ID system, but complex challenges in dealing with how private sector can use it

Thailand

[ADPL Ch12 'Thailand – ASEAN's incomplete comprehensive laws']

- *Context:* Unstable alternation between military regimes and democracy since WWII; Military and Bangkok elite coup 2014; military junta has announced plans for elections mid-2019.
- APEC and ASEAN member, not OECD
- Current protections negligible
  - Constitutional protection since 2007 of 'a person's family rights, dignity, reputation, and the right of privacy' - ineffective
  - Official Information Act, 1997 – Only covers State; administered by Official Information Commission (OIC); *Unenforceable* privacy principles. Sidelined
  - Some industry sectoral requirements (eg telecomms)
- Succession of failed data privacy bills since 2005, including 2014 authoritarian Bill by the current junta (post-GDPR enlightenment)

63

Thailand – 2018 Bill

- **Further Update** pp. 10-11
- Draft *Personal Data Protection Bill* 2018
  - Cabinet approval; public hearings Sept 2018
  - Explicitly aimed at high level of GDPR compatibility
- See lists of key strengths and weaknesses p.11
- New redraft makes it even more GDPR-like
  - But also adds wholesale police/security exemptions
- Major weaknesses (from an 'adequacy' perspective):
  - Confusing and non-independent DPA; lack of appeal
  - Public sector access exceptions? (*Schrems* danger)
  - Data export/onward transfer rules are to be set by DPA
  - Inadequate administrative fines

Result: Best Thai Bill yet, but will need adequacy negotiations

Indonesia

[ADPL Ch 13 '…Indonesia – ASEAN's sectoral laws']

•*Context:* Since 1999 and the end of the Suharto era, a successful democracy with improving rule of law. The largest Muslim Majority country.

•APEC, ASEAN and WTO member

•Implied Constitutional protection (A 28G(1)) has resulted in surveillance requiring legal regulation

•Public Information Disclosure Law (2010) establishes a right of access (but not correction) to government files

•Information and Electronic Transactions Law 2008

- Highest form of Indonesian legislation
- A26 requires consent for use of any person's personal data 'by use of electronic media' – a 'broad brush' right; might apply to all sectors
- 'Elucidation' implies rights of access and correction
- A26(2) Courts can award compensation for breaches (No cases yet)

65

Indonesia – 2012 & 2016 Regulations

- 2012 Regulation on Operation of Electronic Systems and Transactions A15
  - 2nd highest form of Indonesian legislation; Scope of 'Electronic Service Organisations' (ESO) may apply to both private and public sectors (unclear)..
  - Definition of 'personal data' is broad; unsure if excludes publicly available data,
- 2016 Ministerial Regulation on Personal Data Protection in Electronic Systems strengthens rules – see *Update* p31, article by AA Rahmin
- Together, Act + both Regulations go well beyond OECD basic privacy principles:
  1. 'Secrecy, integrity and availability' (2012)
  2. Collection and use based on consent, or legal authority (2012)
  3. Disclosure based on consent, in accordance with purpose of acquisition disclosed at time of acquisition (2012))
  4. Data breach notification requirement (2012): Must notify data subject; + regulatory agency if effects serious (2012)
  5. Security requirements (many provisions); cerification of systems rquired (2016)
  6. Access and correction (2008 Law)
  7. Right to be forgotten (2016 amendment to 2008 Law)
  8. Data exports require Ministerial approval; some data localisation requirements (2016)
  9. Ministry-based complaints system for data breaches only (2016)

Result: Significant principles but ineffective due to absence of a DPA

66

Indonesia - Enforcement

- Breaches of A15 can result in administrative sanctions (fines) & service suspensions
- A26 of 2008 law provided right to sue for compensation (also perhaps under Civil Code)
- No criminal penalties for A 15 etc breaches
- 2016 Reg complaint system only applied to data breaches
- Data localisation: ESOs must locate 'data centre and disaster recovery centre' on Indonesian territory (A 17)
- 'Reliability Certification Agencies' (A 68) could become relevant to APEC-CBPR
- Lack of a separate DPD minimises effectiveness

67

Indonesia – 2018 Bill

- Kominfo draft *Data Protection Bill* (April 2018)
  - There are different versions in circulation
  - Little likelihood of 2018 enactment; EU assistance
- See lists of strengths and weaknesses (**Further Update** p.12)
  - Comprehensive scope
  - All basic principles + some GDPR-influenced; many GDPR principles absent, but uncertain how essential they are
  - Data export restrictions based on 'equal or higher' law of recipient country + White List
  - DPA (independence uncertain) with strong powers including supervising mediation; compensation; administrative penalties up to US$2M; criminal offences
- Result: Would be one of the stronger Asian laws if enacted, but would require adequacy negotiations, particularly re independence
  - Has to co-exist with localisation requirements

References

- My home page contains links to most of my papers http://www2.austlii.edu.au/~graham/
- More easily found on my SSRN page at http://ssrn.com/author=57970
- *Privacy Laws & Business* website has links to many Data Protection Authority home pages http://www.privacylaws.com/Links/

69

Wrap up

1. Build awareness of local developments and nuances
2. Partner with local teams and reinforce a data protection culture
3. Be clear on your must haves and thoughtful in design