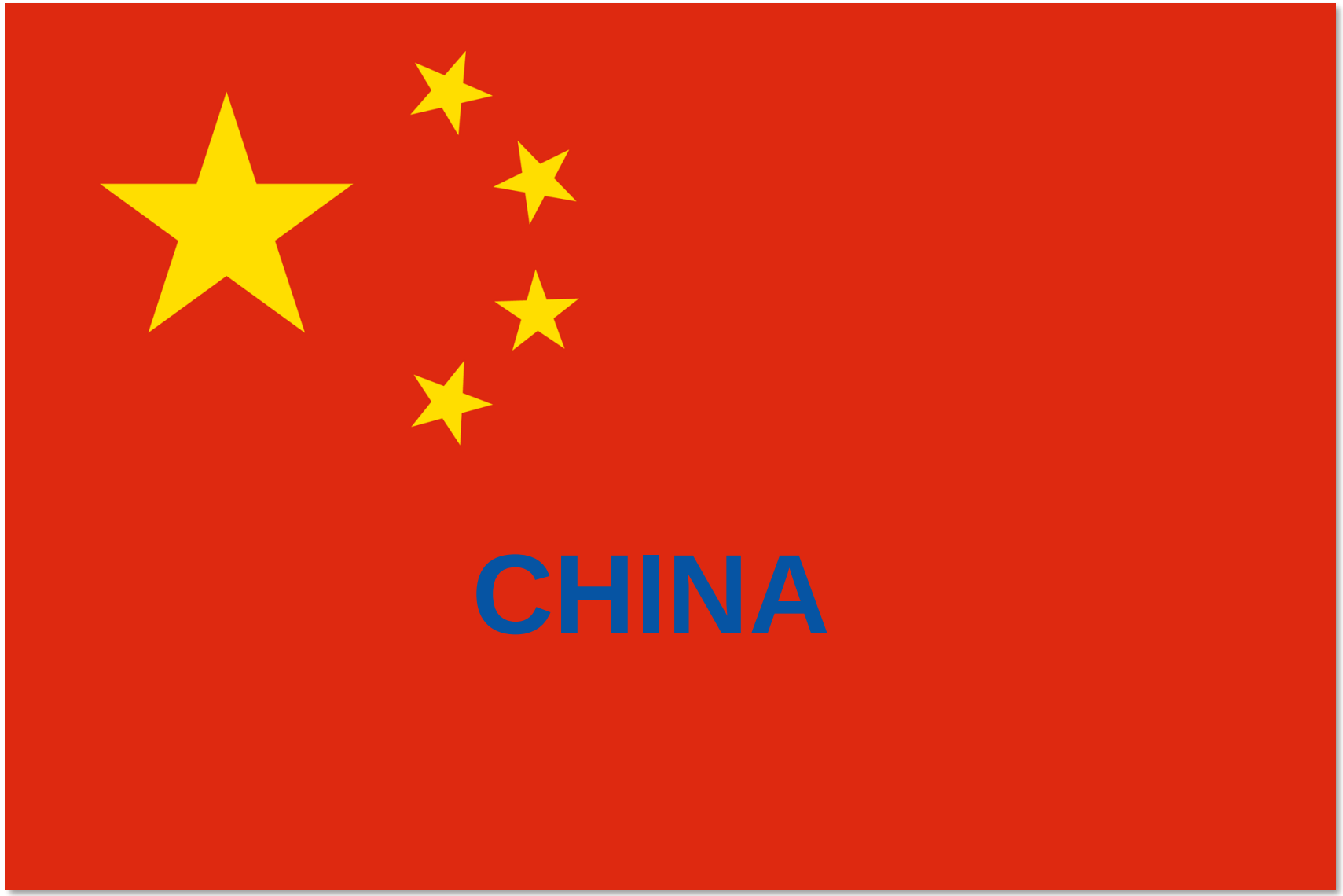

CHINA

Part 2 – China

Timetable of PRC legislation

Key data protection rules

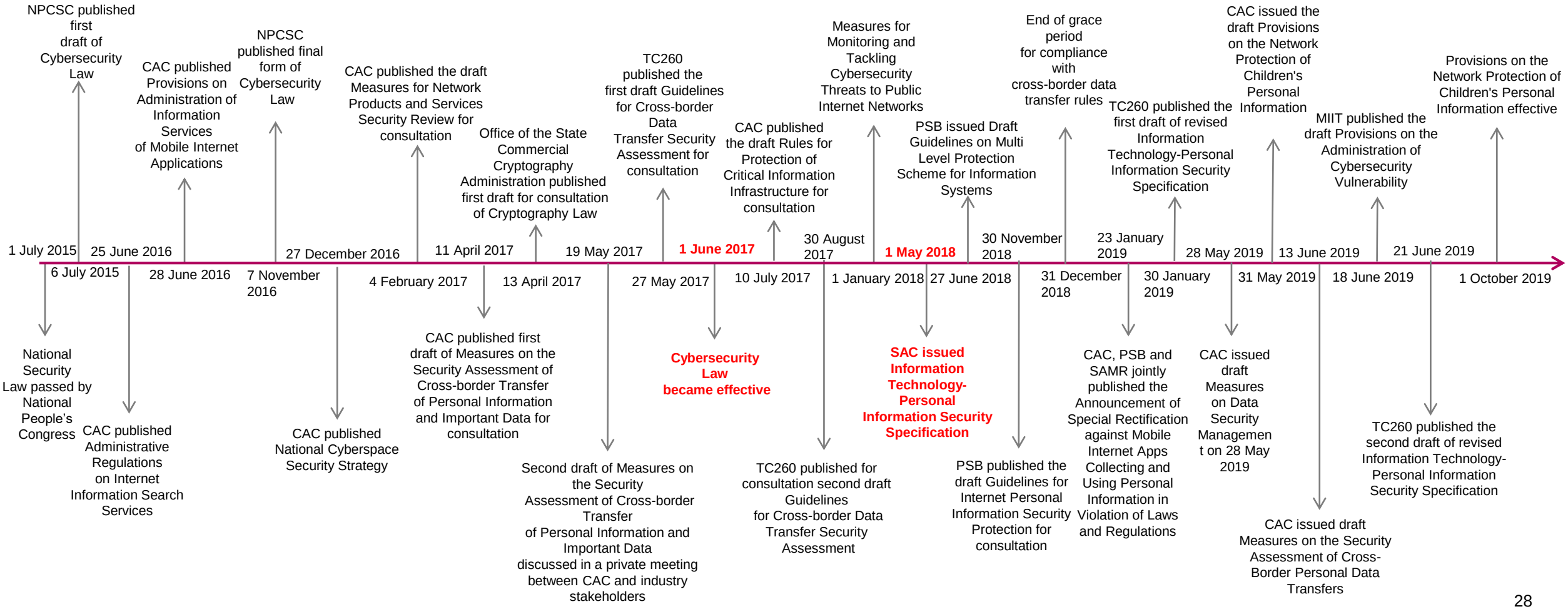
Processing conditions

Cross-border data transfers

Rights of data subjects

Enforcement

Timetable of PRC legislation



Key data protection rules

Cybersecurity Regime

- **Legislative technique**
  - Personal Information and Important Data Protection System **4th of 6 pillars**
  - **GDPR primary model**; Chinese application
- **Legislative objective**
  - **Political** backdrop key
  - Strong focus on **cybersecurity**
  - Data flows are **national resource**
- **Focus**
  - Protection of **network infrastructure**
  - **Extensive scope**, also addresses data protection
- **Flexibility**
  - **Permissive** and (arguably) **flexible**
  - **Room for interpretation** for enforcement

PRC Cybersecurity Law

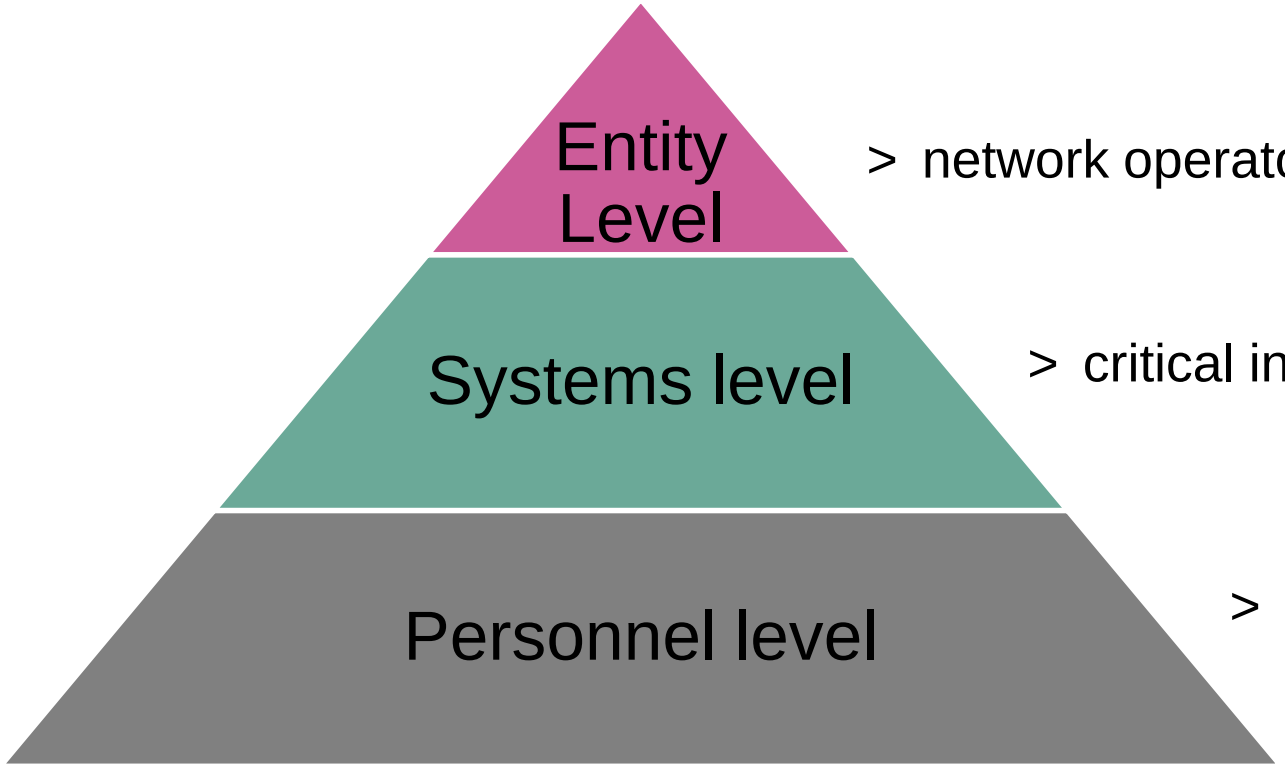
- Mandatory law: framework to be filled out by implementing legislation
- Scope of application: relevant operators and types of data
- Cybersecurity compliance obligations
- Cross-border data transfer restrictions
- Data breach reporting
- Sanctions

Information Security Technology - Personal Information Security Specification

- 1 May 2018 (and revised draft proposals in 2019)
- Issued by China´s main standards body (TC260 = National Information Security Standardisation Technical Committee)
- Best practice guidance but expectation of compliance
- Principles heavily influenced by GDPR

Scope of regime

Analyse via different levels of an organisational structure:



> network operators and service providers

> critical information infrastructure

> individual staff positions

Applicable operators

Network operators

> Owners and administrators
> Computer systems and related equipment
> **In PRC**

CAC clarified that definition of NO should apply if:

- "conducting business operations" or
- "providing services"

Guidance on applicability:

> **Offshore entities** providing cross-border services to **onshore clients**:

Non-exhaustive list of factors to consider

> **Onshore entities** providing services solely to **offshore entities** or third parties:

Yes, but in context of cross-border data transfer must assess if in-scope transfer

Critical information infrastructure operators

Scope of definition remains unclear:

Refined 2 limb test under draft CII Rules: (1) Industry and (2) Impact of system failure

In-scope data types

Personal information

- "Personal information" refers to various information which is recorded in electronic or any other form and (i) can be used alone or in conjunction with other information to recognise the identity of a natural person, including the name, date of birth, ID number, personal biological identification information, address and telephone number of the natural person, or (ii) reflects the activities of specific natural persons including account passwords, asset status, behaviour and location.
- Categories of personal data under Specification include (NB not mandatory application):

Sensitive personal information

- "Sensitive personal information" refers to personal information of which leakage, illegal provision or abuse may endanger the safety of life and property and personal information, such as personal reputation, physical and mental health damage, or discriminatory treatment can easily be caused.

Important data

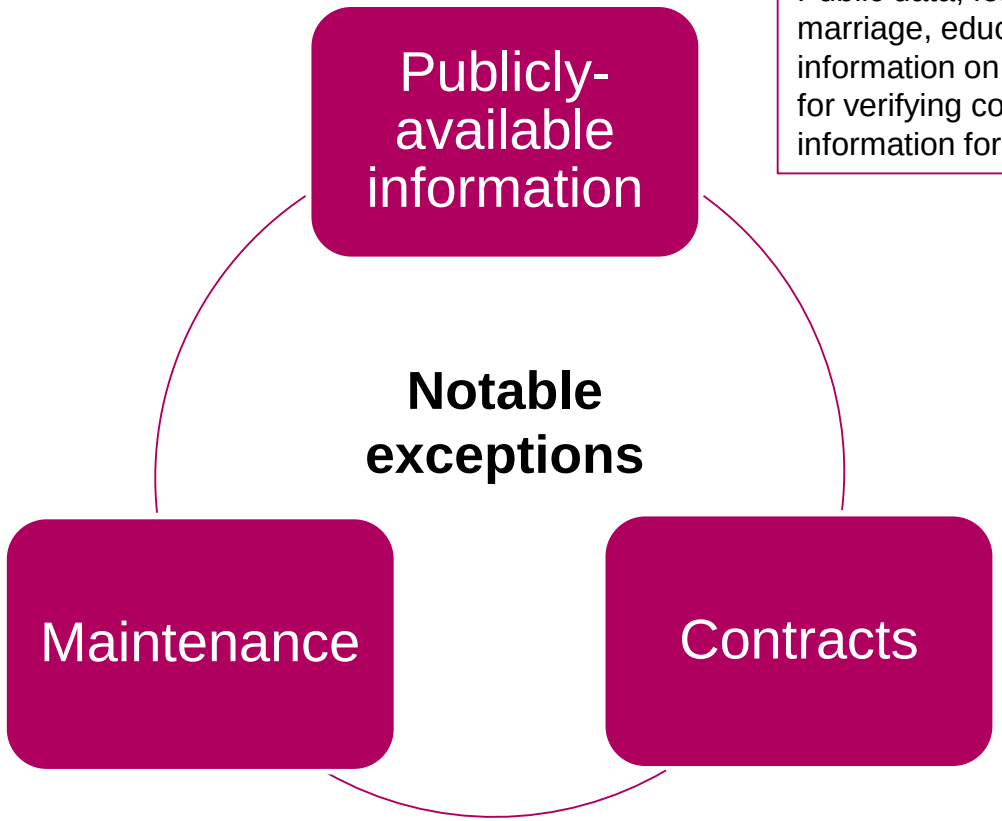
- "Important data," refers to data that, once divulged, may lead to direct consequences in relation to national security, economic security, social stability or public health and security (such as non-public government information, information on large-scale population, genetic health information, geographic information and information relating to mineral resources, etc.) but usually does not include information related to the production and operation and internal management of enterprises or personal information.

Processing conditions

Consent is core processing condition in the PRC

- Before collecting and processing personal data, must obtain consent
- Consent understood to include implied consent (other than in the case of collecting sensitive personal information)
- Suggested examples include:
  - Acts initiated by data subjects, such as making international phone calls, sending emails or instant messages to individuals or organisations overseas
  - Making cross-border transactions online

To maintain the safe and stable operation of products or services provided to data subjects such as through discovery and dealing with any breakdown/malfunction of these products or services, e.g. activities such as installing patches and security updates to office systems



Public data, for example, birth, marriage, education and other information on public record/websites for verifying counterparty/employee information for compliance purposes

Data is necessary for the signing and performance of a contract in accordance with the requirements of the data subject, e.g. job candidate information to prepare an employment contract

But likely subject to change given proposed changes released…

Cross-border data transfers

"Network operators"	*"Critical information infrastructure operators"*
Collection, processing and transfers of "personal information" require informed consent	Transfers of "personal information" or "important data" only permitted if informed consent AND • "business need" and • strictly-controlled security assessment completed

Exception: data processed so identity of data subject cannot be distinguished and cannot be restored

> Negative feedback: US and others raised concerns at World Trade Organisation
> Legislative direction: some relaxations from first draft showed regulators were listening to industry players

BUT latest draft regulations propose:

> to require prior security assessment and regulatory approval for all personal information and important data cross-border transfers

> to extend restrictions to all network operators

Also:

> requirement to keep records for 5 years in case regulatory inspection

> annual reporting obligation to provincial-level regulator

> "model clause" contractual terms must be put in place with offshore recipient

Rights of data subjects

Regime	Subject access right	Right to rectification	Right to data portability	Right to object	Right to restrict processing	Right to erasure
Cybersecurity Law	(-)	(+)	(-)	(-)	(-)	(+)
Cybersecurity Law + Specification	(+)	(+)	(+)	(+)	(-)	(+)
GDPR	(+)	(+)	(+)	(+)	(+)	(+)

Enforcement

Sanctions / Penalty:	Highest fine 10 times illegal gains; other sanctions e.g. suspension of licence, detention

- Apparent enforcement trend being led by CAC
- Particular focus against domestic enterprises in consumer-facing sectors
- Other enforcement campaigns relating to online apps

> allowing illegal messages to be posted and disseminated on their platforms

> 0.12 billion pieces of hotel record and personal information leaked

> fake news and spreading rumours

> examination of users' consent to intended collection of users' personal data

Business' view…

"*The Cybersecurity Law (CSL) was drafted in 2017... The regulations are still incomplete and stipulations vary from one draft to another, … As they stand, however, they pose an array of issues to both British businesses and the wider business community.*

Perhaps the most critical of these is the data localisation regulation… Multinational companies rely on their global IT systems to share information, increasing collaboration and efficiency as well as synchronising business functions such as finance and human resources. Compromising this connectivity would stunt operations across sectors…

Businesses have found it difficult to prepare for the CSL due to the lack of clarity and transparency… This causes widespread confusion among both local and foreign firms, and compounds compliance costs…. Regulatory terms are often vague, leaving interpretation to the enforcing authority and implementation open to inconsistencies, as well as making it difficult for companies to execute due diligence and compliance"

British Chamber of Commerce in China, Position Paper 2019

Cybersecurity and IT restrictions #1 issue

Key take-aways

Proactivity encouraged rather than “wait and see”

Raise concerns:

- Authorities are listening
- Use appropriate lobbying channels

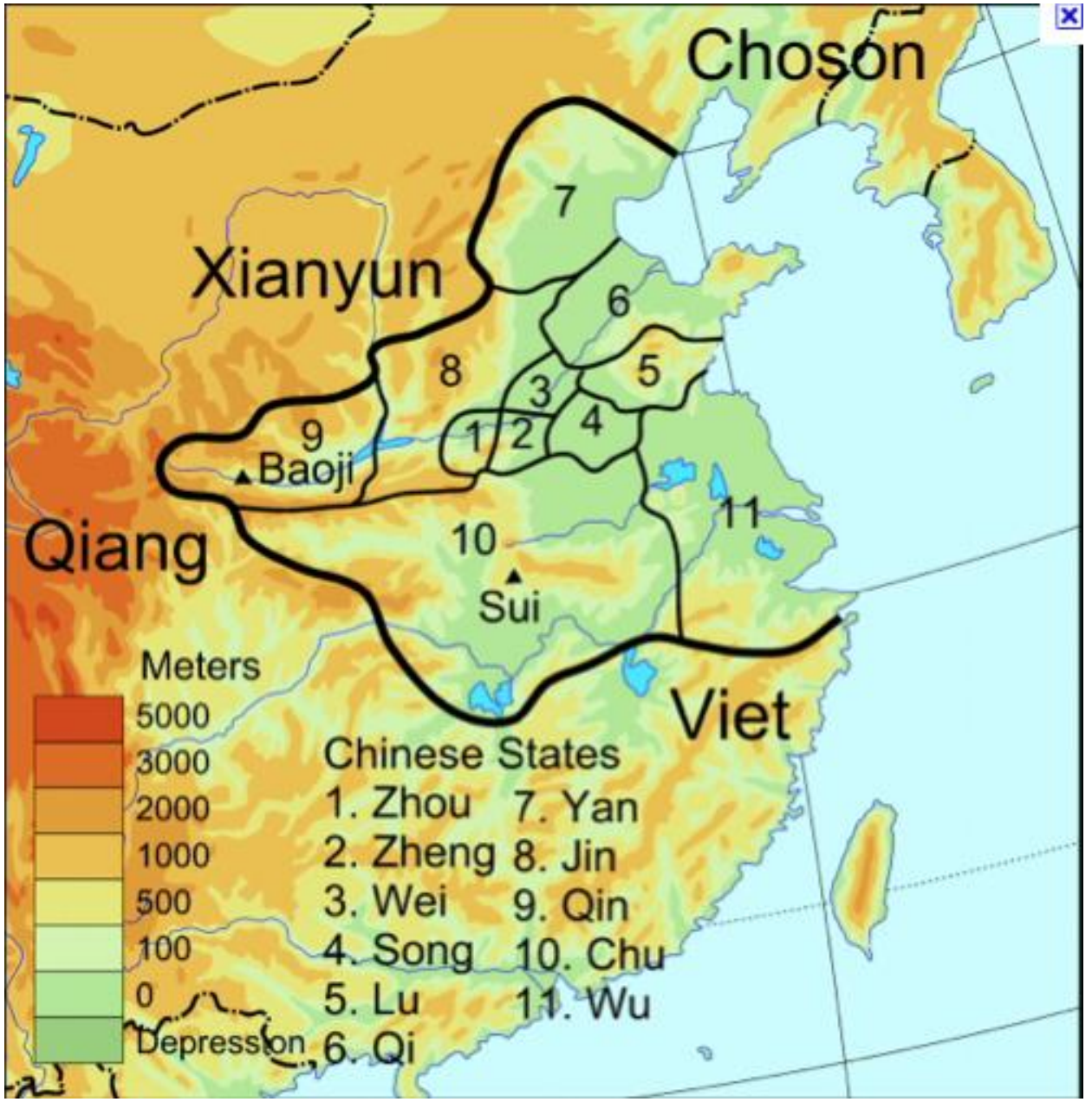
Mind-set of technical and legal teams needs to be:

- Collaborative
- Flexible

Plan ahead rather than take reactionary action

- Take advantage of perceived delays caused by trade war and closely monitor releases of rules
- Assess data flows and services in context of location of customers and other data providers/recipients

China



Map of China in the 'Warring States' period

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
  - This is necessary to increase trust in e-commerce and e-governance within China.
- 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; (ii) the extent of their consistency; and (iv) their implications data transfers to and from China.

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/counter-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
  - Cyber-security regulations to prevent disclosure/export of data.

– 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; now generalised)
  - Rejects multi-stakeholder processes in favour of governments

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

China – Regulation time line

From 2006-10: Uncertain pre-history

1. 2006/7: Draft *Personal Information Protection Act,* from Institute of Law; private & public sectors; included DPA; EU-influenced
2. Some *Province*s 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*

From 2011 – 14: Series of largely consistent limited laws

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

Since 2016: Incomplete new series of laws based around Cybersecurity Law

9. 2016 Cybersecurity Law – most comprehensive & broadly applicable law yet
10. 2018 E-commerce law – wide scope and right of access
11. 2018 Personal Information Security 'Standard' (not a law but treated as such)
12. 2018 draft Ministry of Public Security (MPS) Regulations on 'graded security' & DBN
13. 2019 Measures on …Cross Border Transfer – broader than expected
14. Data localisation aspects of 'Measures' still not complete
15. 2019 Provisions on Cyber-protection of Children's Personal Information

Completion? - Personal Information Protection Law on NPC work program up to 2023

China – Emerging principles in 10+ laws & standards, 2011-19

1. Either (i) 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

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
9. *User rights* are a weakness
   - Correction explicit in CyberSec Law, impled earlier;
   - Access not explicit in CyberSec Law, only in 2018 Standard and 2018 E-commerce law
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, but diverging widely on data localisation and export limits

China – Cybersecurity, data localisation, & export restrictions

- *2019 Update* p6; *Cybersecurity law* (2016); *draft Security Measures* (2017) (withdrawn); draft *Measures on Cross-border Transfers* (June 2019)
- Critical Information Infrastructure (CII) Operators in 2016 law
  - obligations re personal & 'important' data (CII data)
  - But scope of CIIO definition was uncertain
- Two forms of data localisation in 2016 law (attacked in WTO by US/EU) still uncertain because implementing measures not finalised
  1. CII data requires *storage* in 'mainland China' (localisation #1)
  2. Export of some data is *prohibited* (localisation #2)
- Other CII data can be *exported* (localisation #3) only if
  1. export is 'truly necessary' to business; &
  2. security review passed (2019 draft removes self-assessment) &
  3. Data subject consent obtained, after detailed notice.
  4. 2019 draft Measures apply to all transfers of personal information, not only those by CII operators

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

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)

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): 2017 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

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 (2018 Update p. 23)
- *Tort Liability Law* 2009 – 2017 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)

China – Tort law (2)

- *Supreme People's Court Regulations* (2014) 2017 **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.