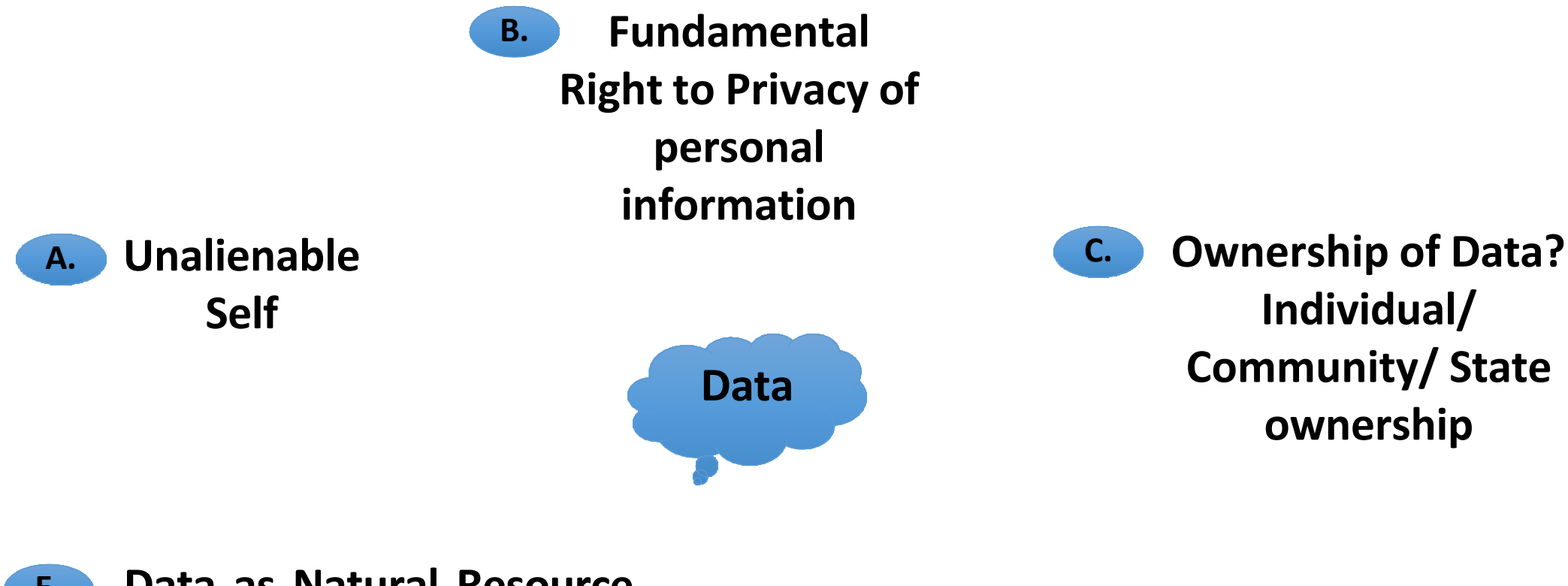
Data Privacy / Protection Framework in US

NALSAR

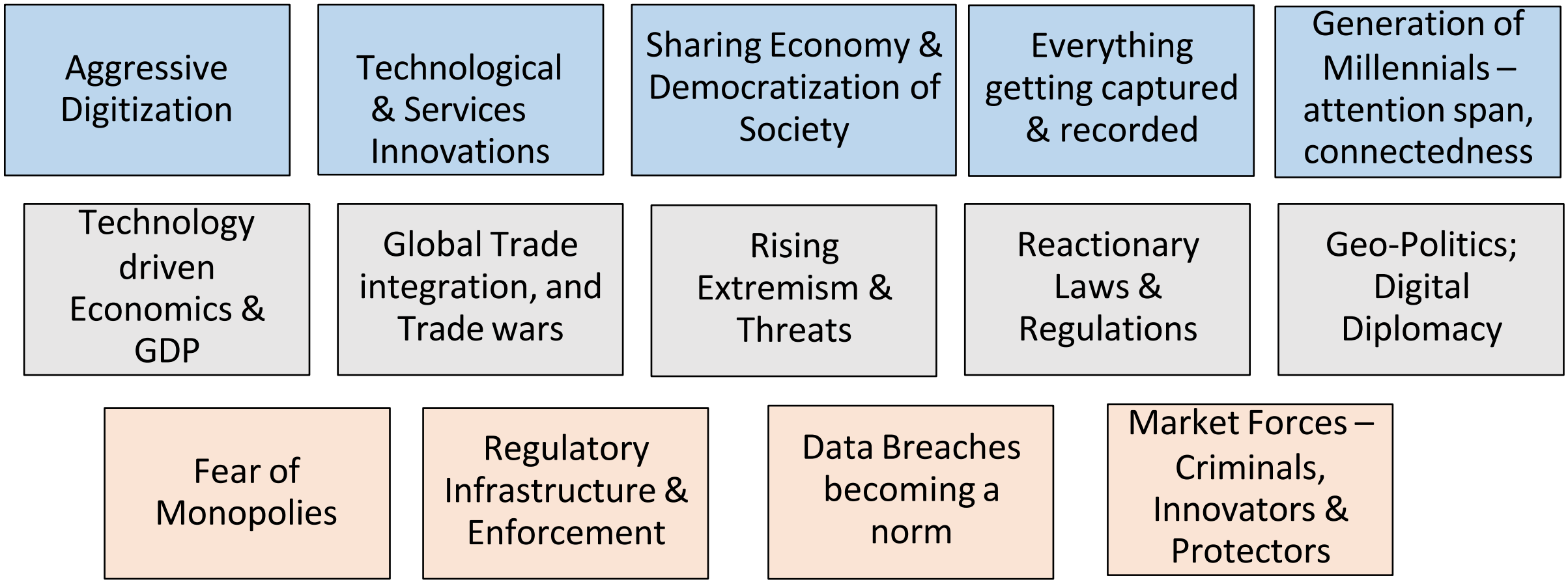
Rahul Sharma
Founder, The Perspective

20th Dec, 2022

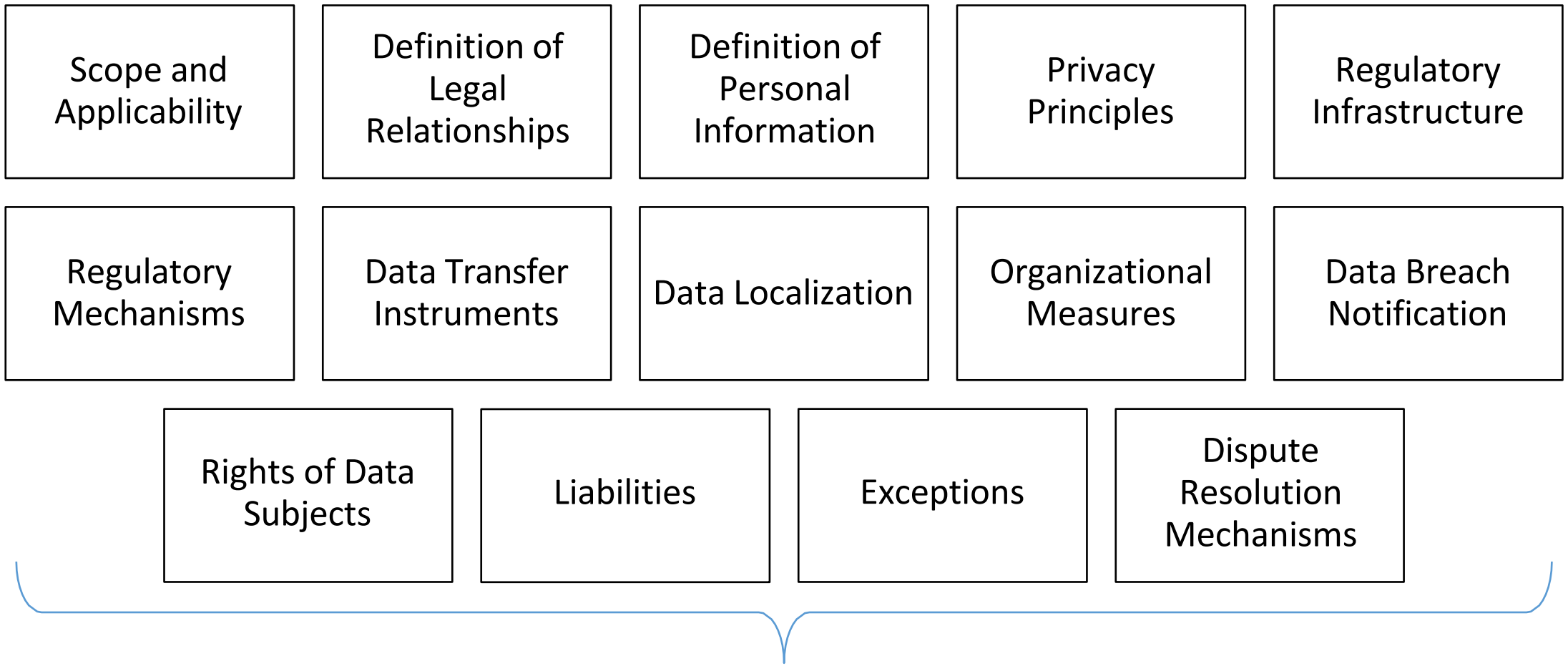
How do we understand Data? Concepts and Analogies



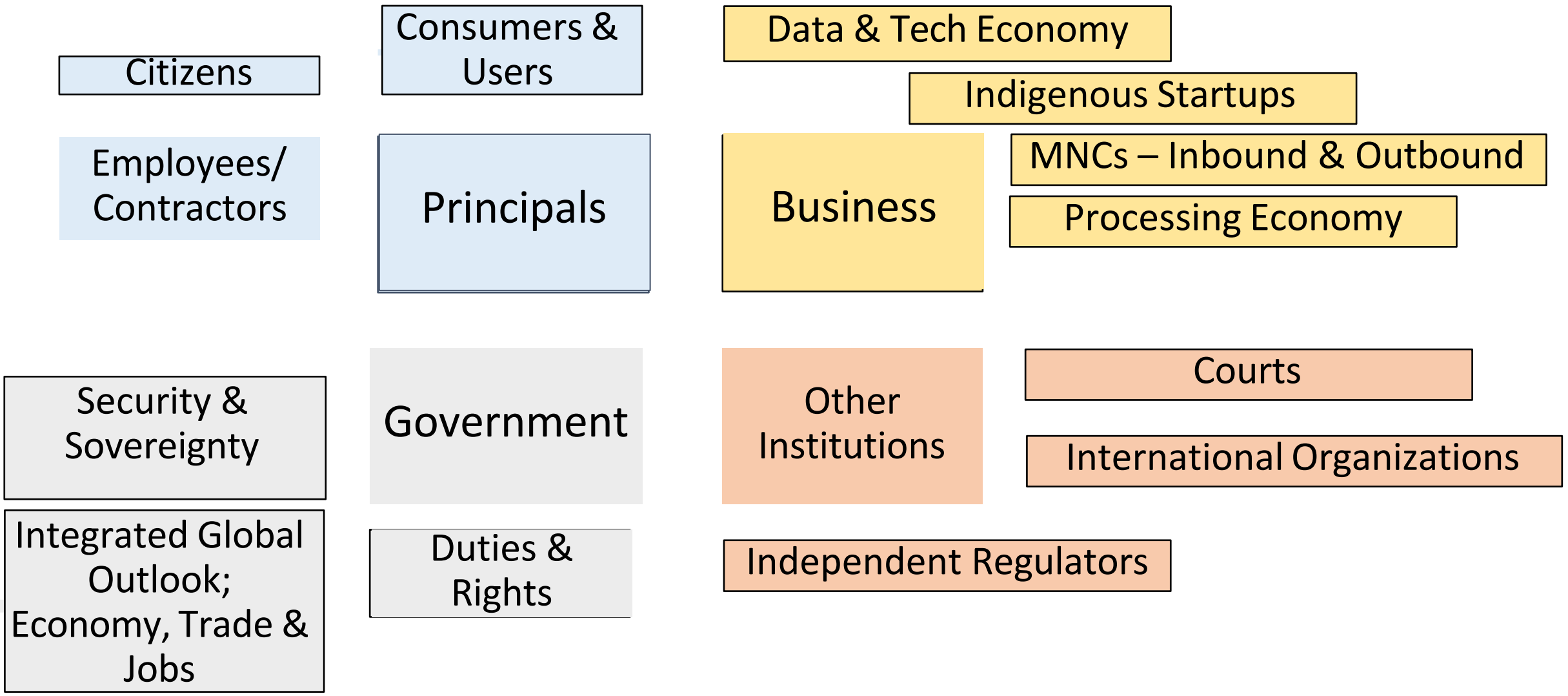
Context of Data Ecosystem



Components of Data Protection Law



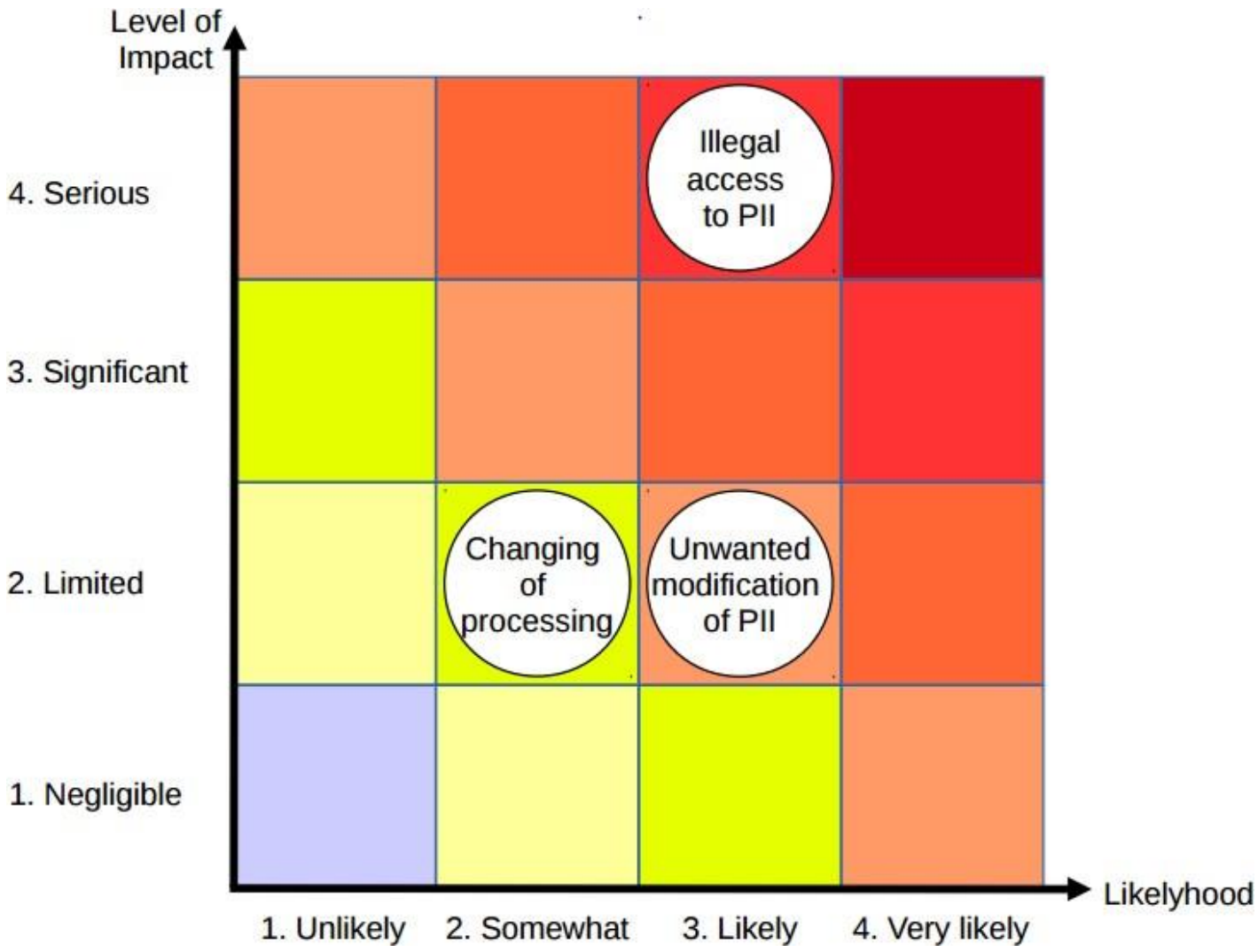
Stakeholders' Perspective(s)



Privacy risks include, but not limited to:

- failure to have the appropriate legal authority to collect, use or disclose personal information;
- excessive collection of PII (loss of operational control);
- unauthorized access to PII (loss of confidentiality);
- unauthorized modification of the PII (loss of integrity);
- loss, theft or unauthorized removal of the PII (loss of availability);
- unauthorized or inappropriate linking of PII;
- failure to keep information appropriately secure;
- retention of personal information for longer than necessary;
- processing of PII without the knowledge or consent of the PII principal (unless such processing is provided for in the relevant legislation or regulation); and
- sharing or repurposing PII with third parties without the explicit informed consent of the data subject

Sample Privacy Risk Map



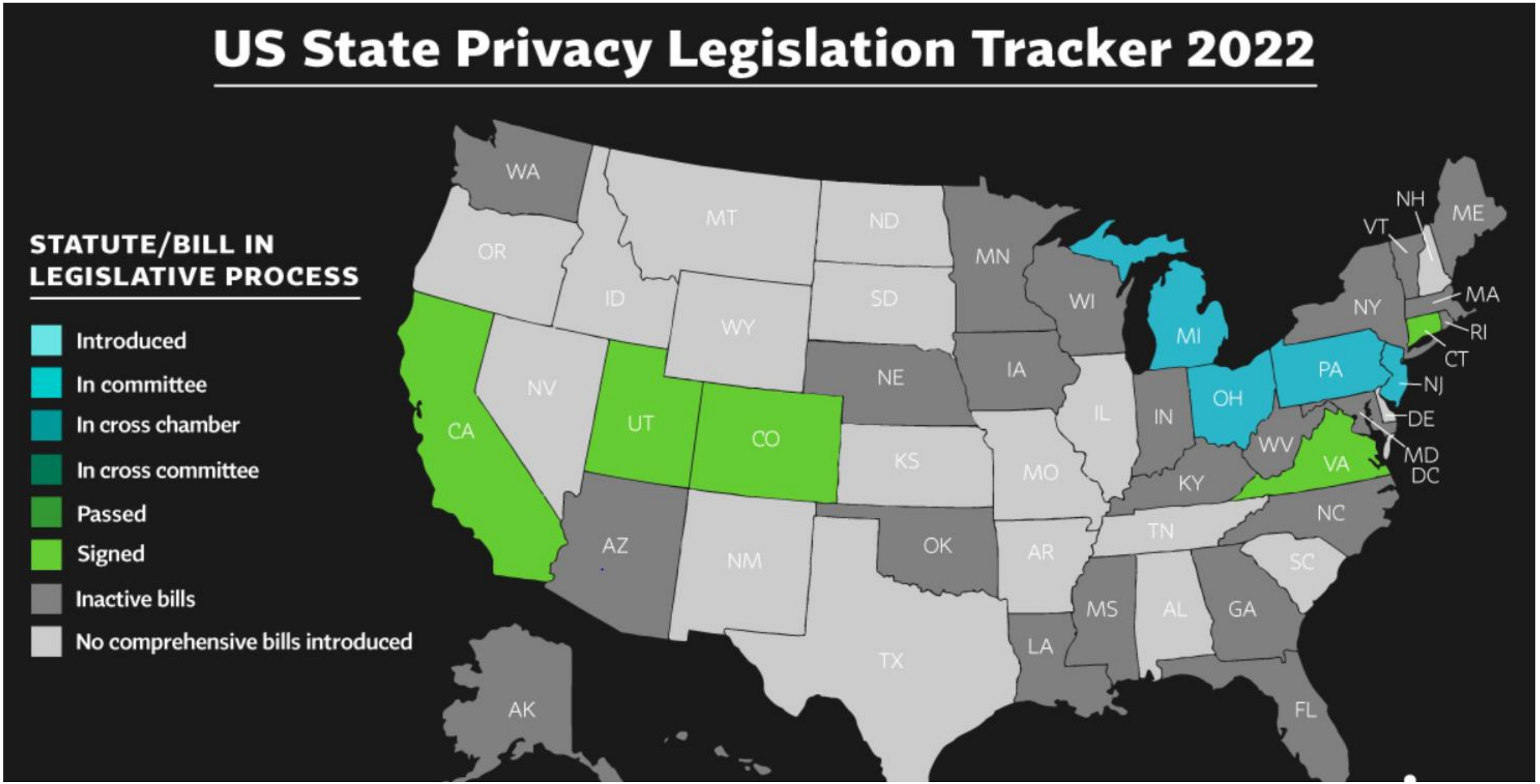
Privacy Assessment Typical Solutions

- deciding not to collect, use or disclose particular types of personal information;
- creating retention periods that only keep information for as long as necessary and planning the secure disposal of information;
- implementing appropriate technological, procedural and physical security measures;
- ensuring that staff are properly trained and are aware of the potential privacy impact and appropriate privacy-protective measures to be followed;
- developing ways to safely anonymize and/or de-identify the information, where possible;
- producing guidance for staff on how to use new programs, processes and systems, and how and when it is appropriate to collect, use, access, disclose and dispose of personal information;
- taking steps to ensure that individuals are fully aware of how their information is used and that they can contact the institution for assistance, if necessary;
- selecting third parties that will provide a greater degree of security and ensuring that agreements are in place to protect the personal information in the custody of the third parties; and
- producing information sharing agreements that clarify what information will be shared, how it will be shared and with whom it will be shared

US Federal Data Protection Framework

- Gramm-Leach-Bliley Act
- Federal Trade Commission Act (Enforcement of Unfair and Deceptive Trade Practices)
- Fair Credit Reporting Act/FACTA
- Family Educational Rights and Privacy Act (FERPA)
- SEC disclosure requirements
- Federal Sector Requirements
  - Federal Information Security Management Act
  - OMB's Breach Notification Policy
  - Veterans Affairs Information Security Act
- Children's Online Privacy Protection Act
- HIPAA/HITECH
- Pending federal bills American Data Privacy Protection Act (ADPPA)
- State Data Protection Laws….

Data Privacy Law Tracker US



Source: IAPP

Data Privacy Law Tracker US

Consumer Right	PIPEDA	CCPA	CPRA	CDPA	GDPR	CPA
Right to access	×	✓	✓	✓	✓	✓
Right to confirm personal data is being processed	×	Implied	Implied	✓	✓	✓
Right to data portability	×	✓	✓	✓	✓	✓
Right to delete ~	×	✓	✓	✓	✓	✓
Right to correct inaccuracies/right of rectification	×	×	✓	✓	✓	✓
Notice and transparency requirements	✓	✓	✓	✓	✓	✓
Right to opt-out of sales	✓*	✓*****	✓*****	✓****	✓**	✓*****
Right to opt-out of targeted advertising (CO and VA) / cross-context behavioral advertising sharing (CA)	×	×***	✓	✓	✓	✓
Right to object to or opt-out of automated decision-making ~ ~	×	×	✓	✓	✓	✓
Opt-in or opt-out for processing of "sensitive" personal data? – "sensitive is defined differently under CPRA, CDPA and CPA	×	×	Opt-out†	Opt-in	Opt-in††	Opt-in†
Right to object to/restrict processing generally	×	×	×	×	✓	×
Right to non-discrimination	×	✓	✓	Limited	Implied	Limited
Purpose / Use / Retention Limitations	×	Implied	✓	✓	✓	✓
Applies to both consumers and in HR and B-to-B contacts	×	+	++	×	✓	×
Privacy and security impact assessments sometimes required	×	×	✓	✓	✓	✓
Obligation to maintain reasonable security	×	✓	✓	✓	✓	✓

2021 PROPOSED FEDERAL LEGISLATION	
Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act (S.2499)	Consumer Data Privacy and Security Act of 2021 (S.1494)

State Data Breach Laws

- There is currently a patchwork of state data breach laws for when information is accessed without authorization. Those breach notification laws often provide specific, and very quick, notification requirements.
- It is important to know where the data subjects are located to understand which laws apply.
- These laws differ with regards to:
  - When you have to notify;
  - Who you have to notify;
  - How you have to notify;
  - Whether there is a private right of action;
  - Whether encryption is a safe harbor; and
  - Whether the law applies to non-electronic data.
- Risk of Harm Analysis
  - Some data breach notification laws allow companies to look at the situation on hand and make a determination on whether the data breach is likely to cause harm to the data subject; if it is likely to cause harm, a breach notification must be sent to affected consumers and vice versa.

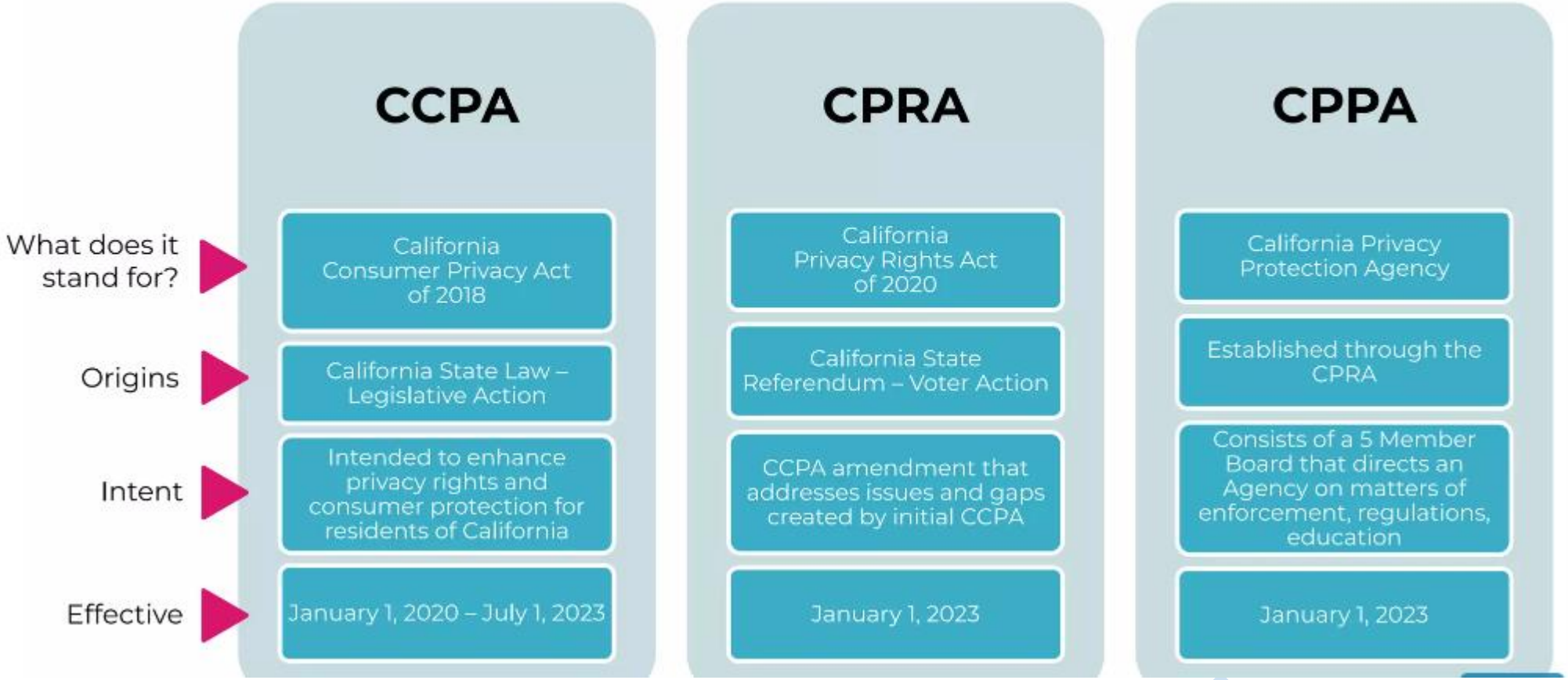
DPIA Legal Requirements - US

Factors Required in a DPIA	CPRA	Colorado CPA 2023	Conn. CTDPA'23	Virginia VCDPA'23
Explain benefits from processing. The DPIA should identify and weigh the benefits that may flow, directly or indirectly, from the proposed processing to either the organization, the data subject, other stakeholders, or the public.	CPRA does not directly require that companies create a DPIA, it empowers the CPPA to issue regulations that might require companies to submit to the agency a risk assessment with respect to certain forms of processing activities	✓	✓	✓
Explain risks from processing. The DPIA should identify and weigh the potential risks to the rights of the consumer associated with the proposed processing.		✓	✓	✓
Describe risk mitigations taken. The DPIA should describe any safeguards that the organization has taken to mitigate potential risks.		✓	✓	✓
Use of de-identification. To the extent that de-identification strategies have been utilized to mitigate risks, those strategies should be indicated.		✓	✓	✓

DPIA Legal Requirements – US

Factors Required in a DPIA	CPRA	Colorado CPA 2023	Conn. CTDPA'23	Virginia VCDPA'23
Reasonable expectations of data subject. The DPIA should consider whether the proposed processing aligns with the reasonable expectations of data subjects.		✓	✓	✓
Compliance with other aspects of state privacy law. The DPIA should consider whether the processing complies with other requirements imposed upon controllers under the state privacy laws.		✓	✓	Attorney General can evaluate the DPIA for compliance with all requirements within §59.1-574

CCPA, CPRA, and CPPA Overview



How is Sensitive Personal Information defined in CPRA

SPI is a subset of personal information newly defined in the CPRA. SPI is personal information that reveals:

- a consumer's social security, driver's license, state identification card, or passport number;
- a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
- a consumer's precise geolocation;
- a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
- a consumer's genetic data.

How is a 'business' defined?

The CPRA defines a "business" as:

- a for-profit legal entity:
  - that collects consumers' personal information on its own or by others on its behalf
  - that alone or jointly with others determines the purposes and means of the processing
  - that "does business" in California
  - and satisfies at least one of the following thresholds:

    i. has annual gross revenues in excess of $25 million

    ii. annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or devices

    iii.derives 50% or more of its annual revenues from selling consumers' personal information

What does 'sharing' personal information mean?

The CPRA defines "sharing" as renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

Obligations

What are the principal obligations of a contractor?

A contractor must:

- use personal information only to perform services on behalf of a business as specified in a contract
- comply with the terms of the contract
- implement security safeguards
- not combine personal information received from a given business with any personal information received from others
- notify the business regarding their use of subcontractors, and those subcontractors must be contractually bound to the same terms as the contractors.

What rights do consumers have?

The CCPA creates six specific rights for consumers:

1. the **right to know** (request disclosure of) personal information collected by the business about the consumer, from whom it was collected, why it was collected, and, if sold, to whom;

2. the **right to delete** personal information collected from the consumer;

3. the **right to opt-out** of the sale of personal information (if applicable);

4. the **right to opt-in** to the sale of personal information of consumers under the age of 16 (if applicable);

5. the **right to non-discriminatory treatment** for exercising any rights; and

6. the **right to initiate a private cause of action** for data breaches.

The CPRA creates two additional rights:

7. the **right to correct** inaccurate personal information; and

8. the **right to limit use and disclosure** of sensitive personal information.

What are the consequences for non-compliance?

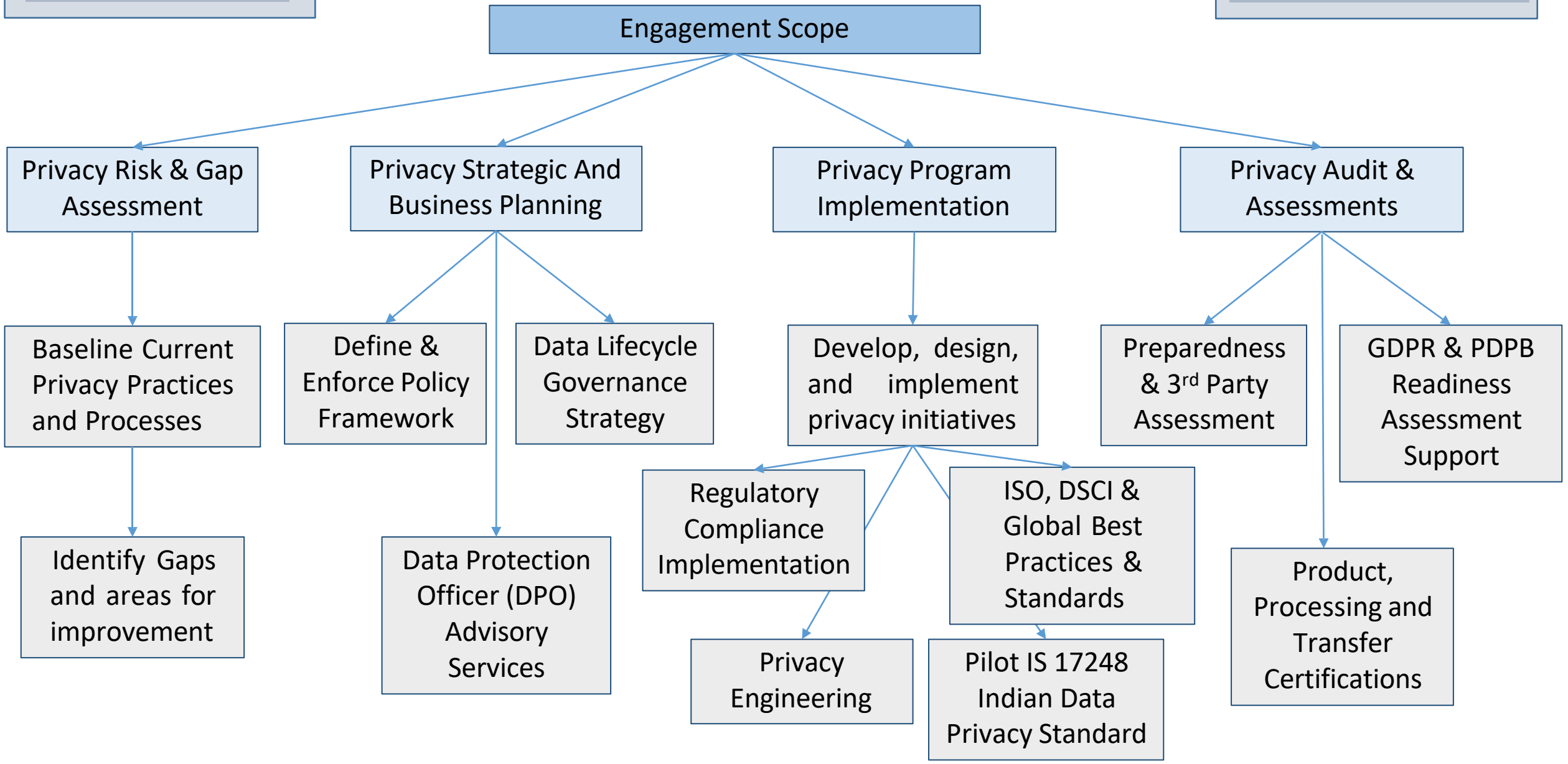
The CCPA provides for the following options for imposing liability in the event of non-compliance:

- Civil Penalties – In actions by the California Attorney General, businesses can face penalties of up to $7,500 per intentional violation or $2,500 per unintentional violation (but there is an opportunity to cure any alleged violation within 30 days after receiving notice of the alleged violation).
- Damages – In actions brought by consumers for security breach violations, consumers may recover statutory damages not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater. In actions for statutory damages, consumers must first provide businesses with written notice and an opportunity to cure.
- Non-Monetary Relief – In actions brought by consumers for security breach violations, consumers may seek injunctive or declaratory relief, as well as any other relief the court deems proper.
- Businesses may also be subject to an injunction in actions brought by the Attorney General.

Privacy - Data Protection Offerings

The Perspective™

Grade Ace Pvt Ltd



Thank You

ThePerspective.Rahul@protonmail.ch;

+91-9711156157

Articles Link:

1. DPDP Bill: Opportunities and Data Protection Balancer https://www.medianama.com/2022/12/223-views-dpdp-bill-2022-opportunity-data-protection-balancing/

2. Contemporising Data Protection Legislation: https://www.orfonline.org/expert-speak/contemporising-data-protection-legislation/