Data Privacy / Protection Framework in US

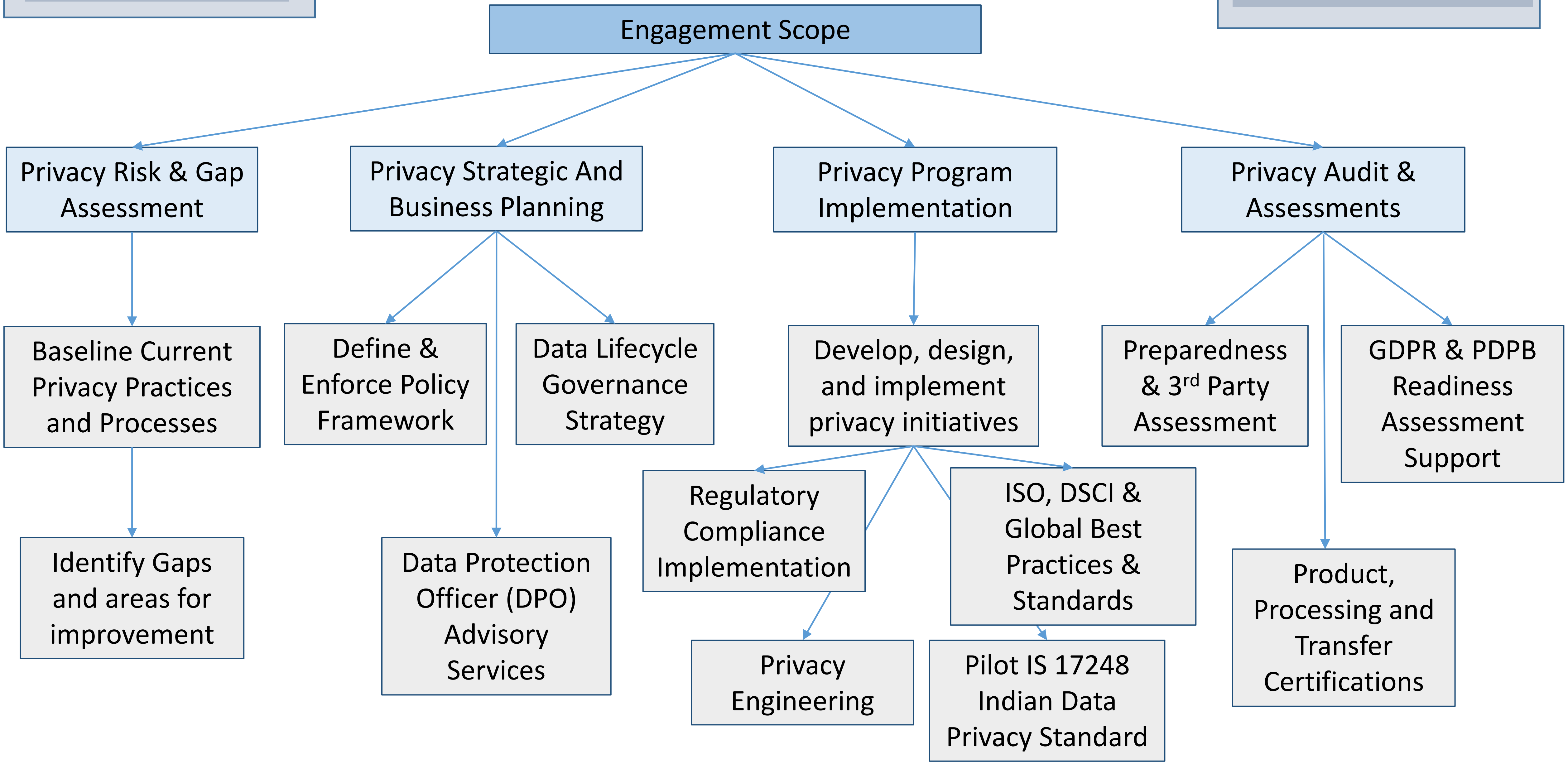
Rahul Sharma
Founder, The Perspective

11th Dec, 2021

Privacy - Data Protection Offerings

The Perspective™

Grade Ace™ Pvt Ltd



How do we understand Data? Concepts and Analogies

Data

A. Unalienable Self

B. Fundamental Right to Privacy of personal information

C. Ownership of Data? Individual/ Community/ State ownership

D. Rights over data akin to property rights

E. Data as Natural Resource acting as fuel (oil/ water/ gold/ uranium) of digital economy

Context of Data Ecosystem

- Aggressive Digitization
- Technological Innovations
- Sharing Economy & Democratization of Society
- Everything getting captured & recorded
- Generation of Millennials – attention span, connectedness

- Technology driven Economics & GDP
- Global Trade integration, and Trade wars
- Rising Extremism & Threats
- Reactionary Laws & Regulations
- Geo-Politics; Digital Diplomacy

- Fear of Monopolies
- Regulatory Infrastructure & Enforcement
- Data Breaches becoming a norm
- Market Forces – Criminals, Innovators & Protectors

Components of Data Protection Law

Scope and Applicability	Definition of Legal Relationships	Definition of Personal Information	Privacy Principles	Regulatory Infrastructure
Regulatory Mechanisms	Data Transfer Instruments	Data Localization	Organizational Measures	Data Breach Notification
Rights of Data Subjects	Liabilities	Exceptions	Dispute Resolution Mechanisms	

ECONOMIC – SOCIAL – ADMINISTRATIVE REGULATION

Stakeholders’ Perspective(s)

Citizens

Consumers & Users

Employees/ Contractors

Principals

Data & Tech Economy

Indigenous Startups

Business

MNCs – Inbound & Outbound

Processing Economy

Security & Sovereignty

Government

Integrated Global Outlook; Economy, Trade & Jobs

Duties & Rights

Other Institutions

Courts

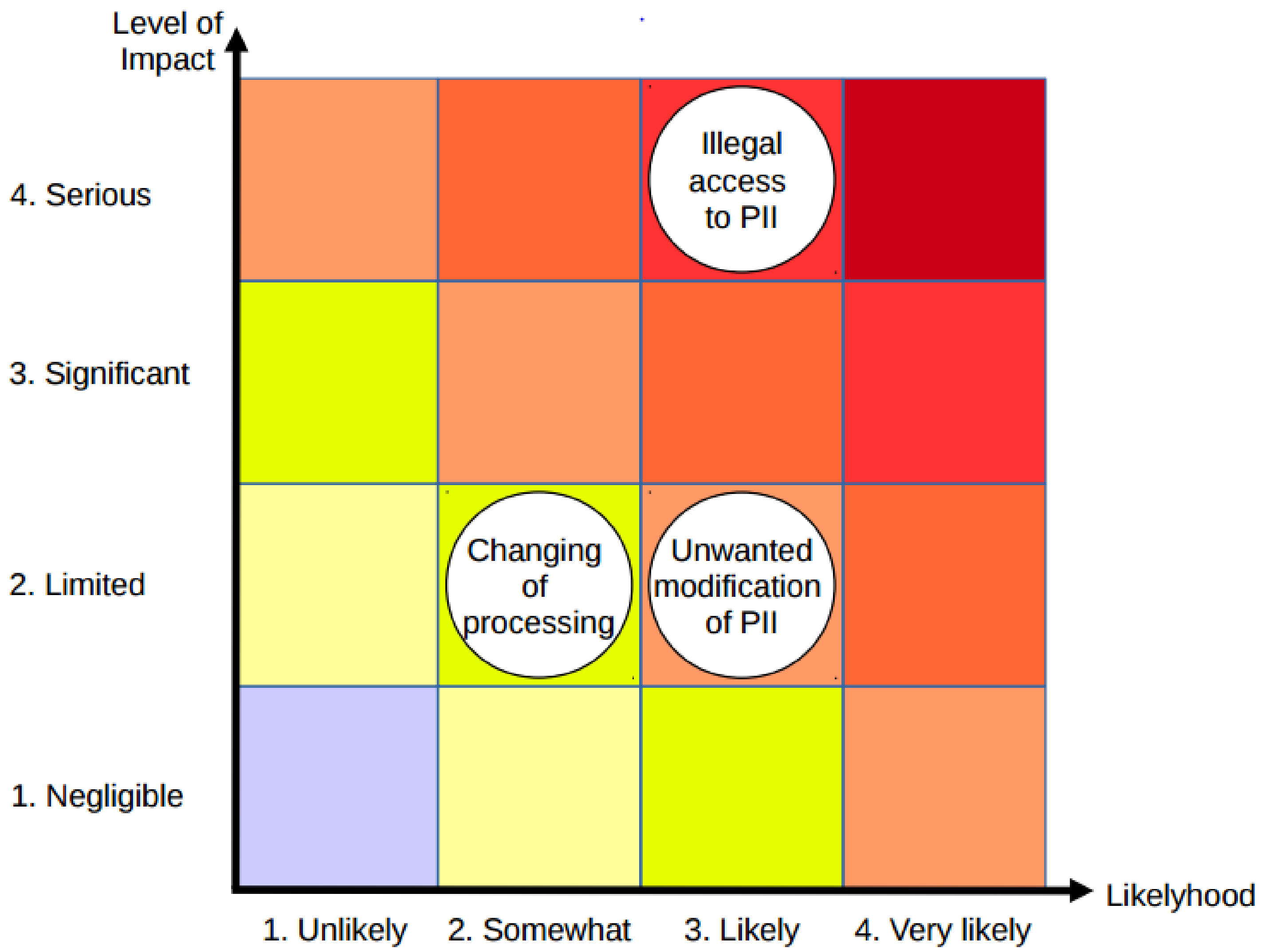
International Organizations

Independent Regulators

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

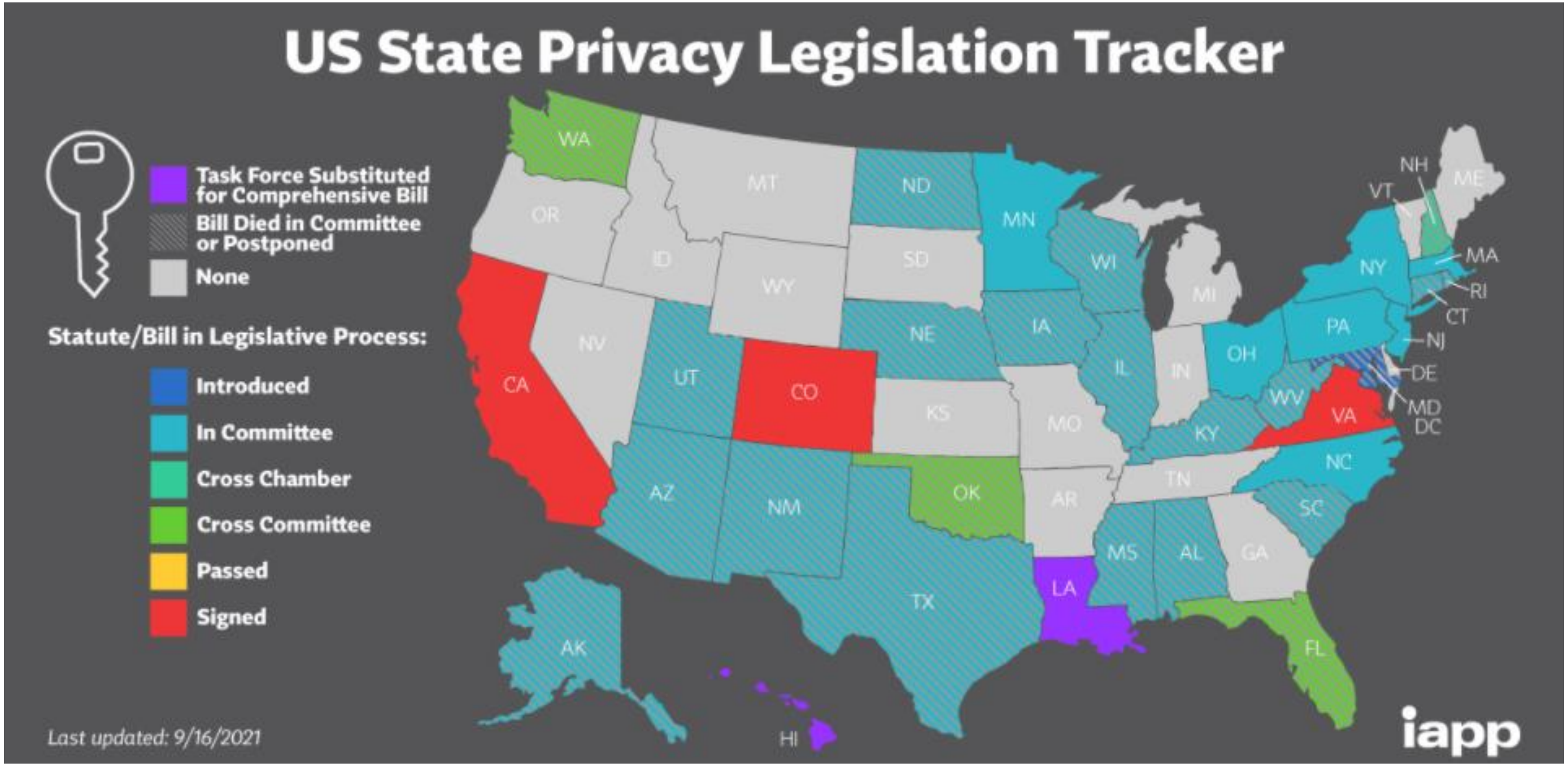
US Federal Data Protection Framework

- Gramm-Leach-Bliley Act
- Federal Trade Commission Act
- Fair Credit Reporting Act/FACTA
- 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

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)

INDIVIDUAL RIGHTS	Right to access
	Right to correct
	Right to delete
	Right to portability
	Right to opt out of all or specific processing
	Right to opt in for sensitive data processing
	Age-based opt-in right
	Notice/transparency requirements
BUSINESS OBLIGATIONS	Purpose limitation
	Data minimization
	Security requirements
	Privacy-by-design/privacy program
	Processor/service provider requirements
	Automated decision-making requirements
	Risk/impact assessments
	Training
	Privacy officer
	Nonprofits covered
ENFORCEMENT	Sectoral law carveouts
	State-level preemption
	Enforcement authority
	Rulemaking authority
	FTC “first-time” civil penalty authority
	Private right of action

Data Privacy Law Tracker US



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.

Thank You

ThePerspective.Rahul@protonmail.ch;

+91-9711156157