16th ACM Conference on Data and Application Security and Privacy (CODASPY) 2026

Local Privacy Laws in a Globalized World

Shantanu Sharma

New Jersey Institute of Technology

Ethan Myers

Colorado State University

Lorenzo De Carli

University of Calgary

Ritwik Banerjee

Stony Brook University

Indrakshi Ray

Colorado State University

The Blindspot in Digital Privacy Research

Personal data

✓ Drives business decisions, advertising, and revenue

⚠ Enables invasive monitoring of users

Digital privacy research relies on a narrow scope of Western regulations

We present a comparative analysis

6 laws, 5 continents, 38.3% world population coverage

Our analysis is based on data lifecycle phases: collection, storage, processing, sharing, deletion, bequeath

The Blindspot in Digital Privacy Research

66.67%

14 out of 21 studies rely solely on GDPR to define threat models

The GDPR Bias

95%

20 out of 21 studies focus entirely on European or North American laws

The Western Bias

38.3%

Global population covered by 6 major privacy laws. Standardizing on a single regional law leaves critical gaps in global threat modeling

The Reality Gap

Six Jurisdictions • Five Continents

LGPD

Lei Geral de Proteção de Dados Pessoais

BRAZIL

DPDPA

Digital Personal Data Protection Act

INDIA

PIPL

Personal Information Protection Law

CHINA

POPIA

Protection of Personal Information Act

SOUTH AFRICA

GDPR

General Data Protection Regulation

EU

CCPA

California Consumer Privacy Act

California (USA)

Fragmented Mandates

Why does this matter?

- GDPR-centric (or region specific) threat models break outside their domain
- Different protected data under all laws
- Breach rules, deletion timelines, consent models all differ by jurisdiction

Research Goals

- Examine how jurisdictions implement data protection through regulatory laws
- An exploratory review of 21 recent digital privacy-focused papers
- Normalize 6 laws via data-lifecycle perspective
- Analyze user rights, organization obligations, and gov. enforcement
- Guide design of globally applicable privacy threat models

On Regulatory Divergences

1

How do differences in user-level legal protections lead to inconsistent legal outcomes for the same digital data collection behavior?

2

How do differences in organizational obligations across data protection laws constrain the design of a unified and technically enforceable data-processing architecture?

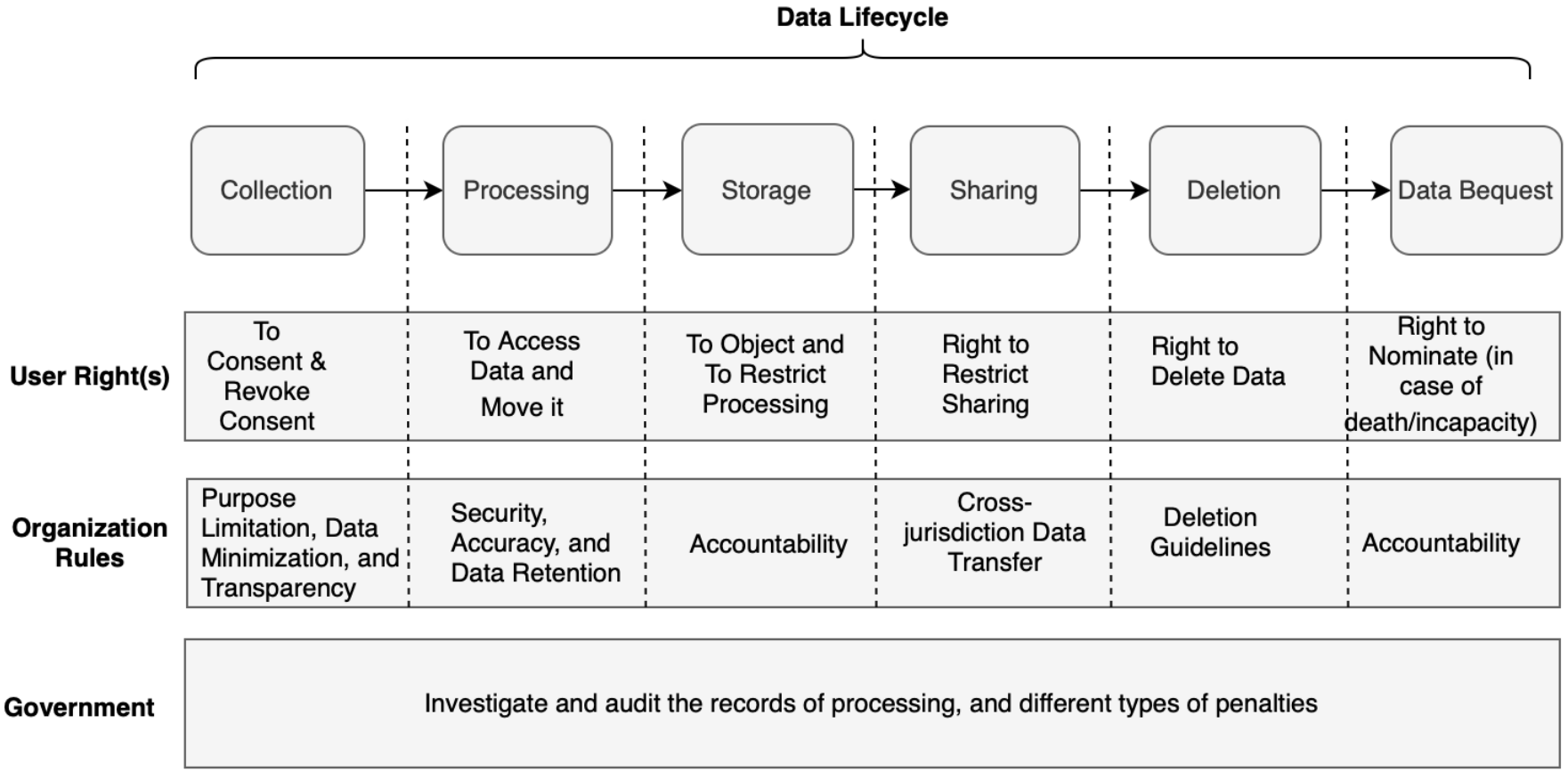
3

How do differences in regulatory oversight and penalty structures result in risks to be faced by developers operating across multiple jurisdictions?

Data Lifecycle Framework

Each law analyzed through

1. Data lifecycle phases
2. Three stakeholder perspectives: users, organizations, and governments



Law Selection

To maximize jurisdiction diversity and maintain analytical depth

- GDPR, the most studied law in privacy research
- Add one law per unrepresented continent
- Prioritize countries with large populations and enacted laws
- Target ~40% world population coverage

User Analysis

How do differences in user-level legal protections lead to inconsistent legal outcomes for the same digital data collection behavior?

Personal Data

Vague and broad:

"any data"
DPDPA, India

"electronically recorded or by other means"
PIPL, China

Fine-grained:

"identified or identifiable person"
LGPD (Brazil) and **GDPR (EU)**

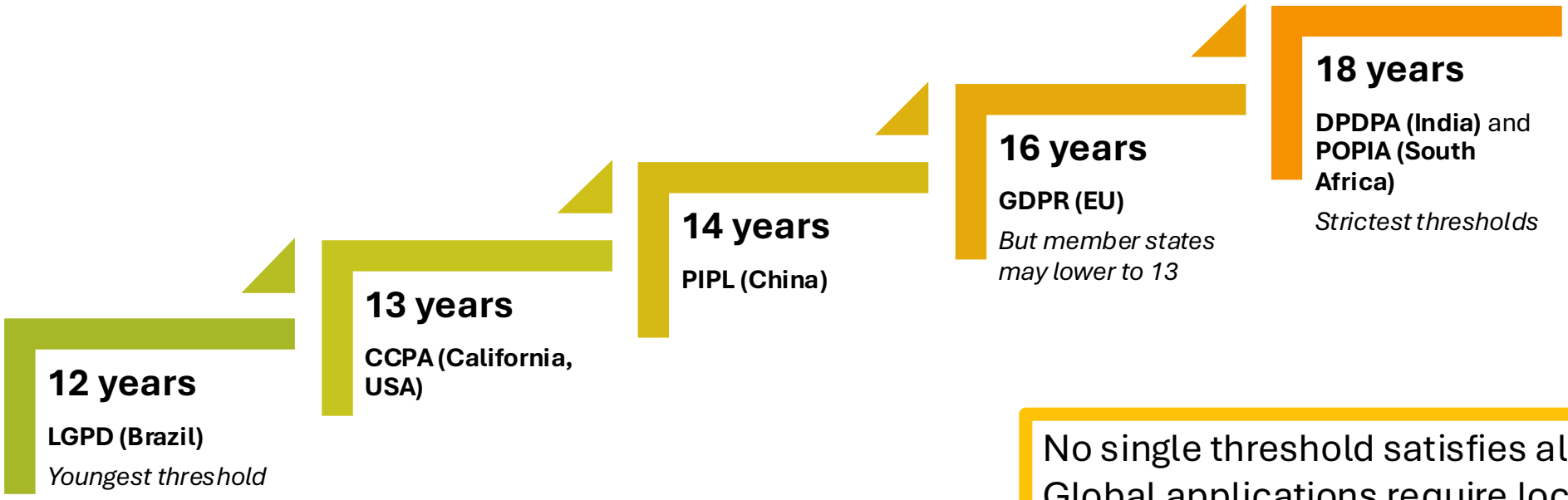
Explicitly includes online identifiers and IP addresses
POPIA (South Africa)

Uniquely expands to include household data
CCPA (California, USA)

User Analysis

How do differences in user-level legal protections lead to inconsistent legal outcomes for the same digital data collection behavior?

On Children



No single threshold satisfies all laws. Global applications require localized logic at collection.

User Analysis

How do differences in user-level legal protections lead to inconsistent legal outcomes for the same digital data collection behavior?

Consent Models

- Consent provides legal basis for processing data
  - However, definition, scope, and enforcement differ across laws
- Consent types refers to granularity:
  - General: allows organization to collect/use data for multiple purpose w/o individual approval
  - Specific: narrow scope, purpose linked, and requires user agreement to each processing/collection activity
- CCPA only law which is Opt-out (assumes consent until it is withdrawn)

Law	Opt-in	Opt-out	Consent Type
GDPR	✓	X	Specific
CCPA	X	✓	General
POPIA	✓	X	Context-Dependent
DPDPA	✓	X	Specific
LGPD	✓	X	Specific
PIPL	✓	X	Specific

User Analysis

How do differences in user-level legal protections lead to inconsistent legal outcomes for the same digital data collection behavior?

User Rights

Law	Consent	Revoke Consent	Access	Erasure	Rectification	Object	Nominate a Representative (death or incapacity)	Portability	Non-discrimination
GDPR	✓	✓	✓	✓	✓	✓	X	✓	X
CCPA	✓	X	✓	✓	✓	✓	X	X	✓
POPIA	✓	✓	✓	✓	✓	✓	X	X	X
DPDPA	✓	✓	✓	✓	X	✓	✓	X	X
LGPD	✓	✓	✓	✓	✓	✓	X	✓	X
PIPL	✓	✓	✓	✓	✓	✓	✓	✓	X

Organizational Analysis

How do differences in organizational obligations across data protection laws constrain the design of a unified and technically enforceable data-processing architecture?

Core Processing Principles & Breach Notifications

Law	Purpose Limitation	Transparency	Security	Data Minimization	Accuracy	Accountability	Fairness	Storage Limitation	Breach Notification
GDPR	✓	✓	✓	✓	✓	✓	✓	✓	72 hours
CCPA	✓	X	X	X	X	X	✓	X	Expedient (no defined timeline)
POPIA	✓	✓	✓	✓	✓	✓	X	✓	As soon as possible
DPDPA	✓	✓	✓	✓	✓	✓	X	✓	**No Deadline**
LGPD	✓	✓	✓	✓	✓	✓	✓	✓	**No Deadline**
PIPL	✓	✓	✓	✓	✓	✓	✓	✓	Immediate

Organizational Analysis

How do differences in organizational obligations across data protection laws constrain the design of a unified and technically enforceable data-processing architecture?

Cross Border Transfers

- CCPA is only law in which transfer of data across boarders is not addressed
- Majority of laws require the destination country to have adequate privacy law
- China requires all data leaving the country to be approved by the Government
- India uniquely allows cross border transfer by default

Law	Requirement for Destination Country
GDPR	Adequate privacy law
CCPA	Not Addressed
POPIA	Adequate privacy law
DPDPA	Allowed by default. Indian Gov. may restrict certain countries
LGPD	Adequate privacy law
PIPL	Requires Chinese Gov. Approval

Government Analysis

How do differences in regulatory oversight and penalty structures result in risks to be faced by developers operating across multiple jurisdictions?

Maximum Penalties

- All laws have monetary maximum penalties
  - Ranging from a set dollar amount to a percentage of the organization's annual revenue (whichever is higher)
- POPIA (South Africa) is the only law which also has possible imprisonment

Law	Maximum Penalties
GDPR	€20M or 4% of annual global turnover
CCPA	$7,500 per intentional violations
POPIA	ZAR 10M or **max 10 yrs imprisonment**
DPDPA	₹2.5B
LGPD	2% Brazil revenue or BRL 50M
PIPL	RMB 50M or 5% annual revenue

Government Analysis

How do differences in regulatory oversight and penalty structures result in risks to be faced by developers operating across multiple jurisdictions?

Overseeing Authorities

- ***Regulatory Authority (RA)***: the designated body responsible for law enforcement
- ***Independence (IN)***: indicates whether the authority operates independently or is subordinate to government entities;
- ***Term Duration (TD)***: specifies the length of service for the members of the authority

LGPD (Brazil)

RA: ANPD
IN: Yes
TD: 4 yr.

DPDPA (India)

RA: Data Protection Board of India
IN: Yes
TD: 2 yr.

GDPR (EU)

RA: Supervisory Auth. (per EU state)
IN: Yes
TD: Min. 4 yr.

POPIA (South Africa)

RA: Information Regulator
IN: Yes
TD: Max 5 yr.

CCPA (CA, USA)

RA: CA Privacy Protection Agency
IN: Not Explicit
TD: Max 8 yr.

PIPL (China)

RA: State Cyberspace Administration
IN: No
TD: undefined

Conclusion

- **95% of papers focused on EU or North American laws**
- **Laws share common abstract goals** but **differ in**
  - Consent
  - Data definitions vary widely
  - User rights
  - Organization obligations
  - Enforcement
- **Such differences create risks** for users, developers, and organizations that function globally
  - Non-uniform definitions and vague requirements in privacy regulations contribute to such risks and unsound threat models

Thank you!