



IKIGAI LAW

Emerging issues in data protection law and law enforcement access to data

Vijayant Singh (Principal Associate)

www.ikigailaw.com | vijayant@ikigailaw.com

Overview:

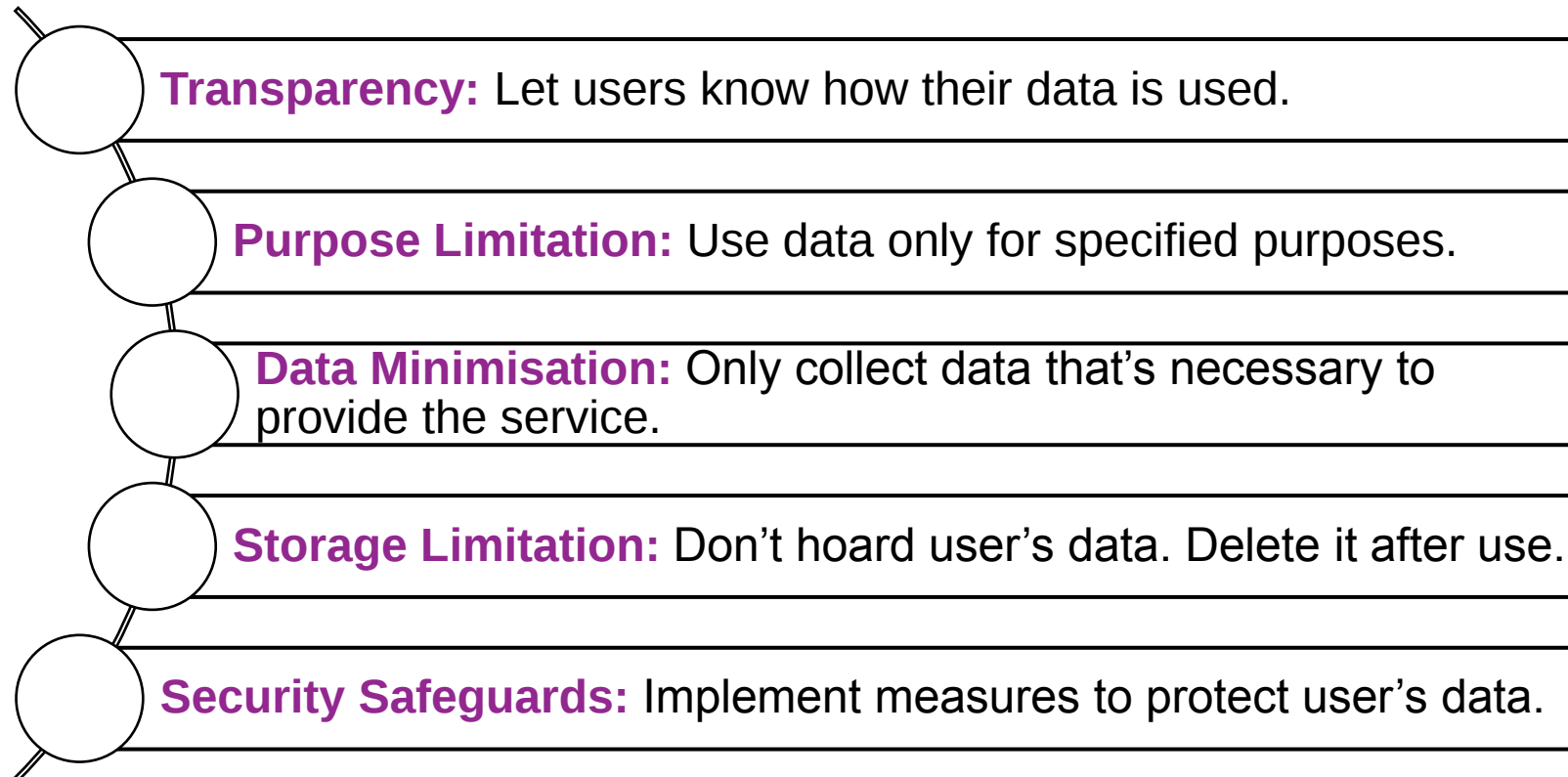


- Overview and context
- How does privacy legislation deal with surveillance?
- What are the challenges under the legal framework for surveillance in India?
- Impact on service providers and technology companies
- Law enforcement access to cross-border data

- State right of surveillance conflicts and intertwines with individual right of privacy.
- The conflict has become more contentious in the age of internet – where all communications are digital and enabled by communication platforms.
- How does surveillance impact fundamental right to privacy and privacy laws?
- Do existing surveillance laws provide adequate safeguards?
- Impact on service providers – ban on end-to-end encryption?
- Cross-border data access to LEAs – challenges with MLATs; solutions like data localization

Digital Personal Data Protection Act, 2023 and Surveillance

- DPDPA, 2023 protects individual rights over personal data and obligates entities that collect data to adhere to rules.
- Applies to government agencies and Indian LEAs.
- Puts general and specific obligations:



DPDPA 2023 enables surveillance

- Section 7(c): allows processing of data without consent if required for performance of state function or for sovereignty and integrity of India
- Section 7(d): allows processing of data without consent if there is legal requirement to disclose data.
- Section 17(1)(c): Limited exemption for data that needs processing for preventing or solving crime.
- Section 17(2)(a): Blanket exemption of DPDPA for government agencies that are notified by central government.

DPDPA 2023: Missed opportunity?

- Possibility to apply certain data protection principles to act of state surveillance – retention limitation; data minimization; security safeguards; purpose limitation etc.
- Exemption power and scope of exemption is overbroad.
- Unclear how this will hold according to Puttaswamy principles and geopolitical considerations of having a strong privacy regime.

India's surveillance framework

- CRPC – Section 91
 - Police or court can seek the production of 'any document or thing' for investigation purposes.
- Telegraph Act:
 - monitoring, interception – covers phone tapping
 - Can be conducted if there is public emergency or for public safety for grounds like sovereignty of India
 - Procedure requires every surveillance order must be approved by a review committee comprising of senior government officials
- IT Act, Section 69 –
 - monitoring, interception, decryption, and also requires 'technical assistance' of service providers
 - No need for public emergency or issue of public safety – provides additional grounds like defence of India
 - Procedure requires every surveillance order must be approved by a review committee comprising of senior government officials
- Additional regulation under IT Act require different service providers to collect or obtain additional data points for law enforcement and national security purposes:
 - Traceability requirement under IL Rules 2021
 - VPN service providers must collect verified customer identity

Challenges of current framework

- No judicial or independent oversight – only executive oversight
- No safeguards like :
 - transparency and reporting requirements
 - internal checks
 - security safeguards
 - Notice to impacted individuals
 - grievance redressal
- Framework challenged in Court as violative of *Puttaswamy* principles of lawfulness, legitimate aim, and proportionality

Impact on communication service providers

- Beyond the law; there is tangible and serious impact on digital platforms that enable communications.
- Most communications take place through such platforms.
- Example: WhatsApp; Zoom; Microsoft Teams; Gmeet; Gmail; Signal
- Privacy v. national security debate is more contentious because of technologies like end-to-end-encryption (E2EE)
- E2EE platforms cannot be surveilled through traditional means of interception, monitoring, and decryption by both digital platforms and government/LEAs.
- LEA problems – ‘going dark’

Legal solutions to account for E2EE

- Mandates for ‘technical assistance’, like in IT Act.
- Mandate to collect additional information, like traceability in IL Rules 2021; user verification obligations in CERT-In Direction 2022, draft Telecom Bill 2022
- Impact of these obligations: break E2EE and redesign platforms?
- Different approaches followed in India, Germany, United Kingdom, Australia, China
- Implications for platform design and privacy and security enabled by digital platforms and technology like E2EE
- Implications for individual rights like privacy, anonymity, confidentiality, and free speech

LEA request for cross-border data

- Indian LEAs need data from service providers located abroad or those that are subject to foreign laws.
- This prohibits Indian LEA access to data.
- Existing mechanisms: MLATs, LRs
- Practical difficulties in accessing data stored abroad – processes are cumbersome, complex, and time-consuming
- Other solutions explored by Indian government – data localization, collecting additional data points, local presence in India
- Potential solution: explore arrangements like CLOUD Act
- Need for surveillance reform



Thank you