PRIVACY ASSOCIATES INTERNATIONAL LLC

Global Privacy Developments

Privacy Law Committee of IT Law Section, State Bar of Michigan

March 21, 2019

Purpose of Session

- Review at a high level some significant developments in Privacy
- General discussion of potential consequences to our companies and clients
- Other privacy topics on the minds of participants

PAI

Subjects for Discussion

- New Brazilian Privacy Law
- Draft Indian Privacy Law
- Chinese Security Rules
- Data Localization Law Metastasis

.

Brazil

Brazil

- General Data Protection Law (LGPD) approved on August 14, 2018, will come into effect after its in early 2020
- GDPR clone, with some differences
- English translation: https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf

Extraterritorial Application

The LGPD applies to companies that:

- Carry out processing of personal data in Brazil;
- Collect personal data in Brazil;
- Process data related to natural persons located in Brazil; or
- Process personal data for the purpose of offering goods or services in Brazil

Personal Data

- Includes any information, whether by itself or in the aggregate, that is relatable to an identifiable natural person
- Sensitive Personal Data includes information on racial or ethnic origin, religious beliefs, political opinions, political opinion, sexual life data, health and other information that allows unequivocal and persistent identification of the data subject, such as genetic data
- Anonymized data is not considered personal data.

Legal Bases for Data Processing

- Done with the express consent of the data subject;
- Necessary for compliance with a legal or regulatory obligation;
- Necessary for the fulfillment of an agreement;
- Necessary for the exercise of rights in a judicial, administrative or arbitration proceeding;
- Necessary to protect life or physical integrity;
- Necessary to protect health;
- Necessary for the implementation of political policies (for processing by the government);
- Necessary for purposes of credit protection;
- Necessary to meet the legitimate interest of the data controller or third parties;
- Necessary for the performance of historical, scientific or statistical research.

PAI

General Principles of Data Protection

Processing must be done taking into consideration certain familiar general principles, such as:

- Purpose limitation
- Necessity
- Transparency
- Security
- Accountability

Data Subject Rights

Examples:

- Right of access
- Right of rectification, cancellation or exclusion
- Right to information and explanation about the use of data
- Right to data portability

Breach Notification

- Must notify DPA within a “reasonable time” after a data breach
  - Definition expected by the data protection authority,
- DPA will determine whether the data subjects must be notified and what mitigating steps must be taken by the company.

International Data Transfers

- LGPD imposes restrictions on cross-border transfers of personal data
- DPA to make adequacy determinations a la EU
- Transfers may be based on consent of the data subject
  - Must be given prior to transfer
  - Consent must be separate from consents for other purposes
- Transfers may be made pursuant to binding corporate rules and standard clauses
- Transfers may be made by means of the adoption of seals, certificates and codes of conduct issued and authorized by the DPA

PAI

Data Protection Officers (DPOs)

- DPO must be appointed by each data controller
  - No GDPR-like exceptions for small businesses or small-scale processors,
  - Possible that the DPA may identify certain exceptions to this requirement in the future
- Is an independent overseer of the company's data protection activities
- Acts as a communication channel between the controller, data subjects and the data protection authority

PAI

Data Protection Impact Assessments

- The LGPD requires companies to generate a data protection impact assessment (DPIA) before undertaking personal data processing activities that may put data subjects at high risk
- The DPIA must document data processing activities that create risks to data subjects, as well as the measures, safeguards and mitigation mechanisms the company has implemented to address those risks

PAI

Record-Keeping

Must maintain detailed records of all personal data processing activities

- Types of personal data processed
- The legal basis that authorizes the processing
- Purposes of processing
- Retention period
- Information security practices implemented
- Sharing of the data

Information Security Requirements

- Both data controller and data processor obligated to take appropriate technical, physical and administrative measures to protect personal data
- The DPA may provide for minimum technical standards, considering the nature of the data handled, the specific characteristics of the treatment and the current state of technology

Penalties

- Fine of up to two percent (2%) of a private legal entity's, group or conglomerate revenues in Brazil, for the prior financial year, excluding taxes, up to a total maximum of R$ 50,000,000.00 per infraction
- Daily fine to the total maximum of R$ 50,000,000.00;
- Publicizing of the infraction
- Blocking of the personal data related to the infraction until its regularization
- Deletion of the relevant personal data

India

- Draft Personal Data Protection Bill, 2018
- English translation: http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf

Application

The PDPA applies to companies:

- Carrying out processing of personal data collected, disclosed or otherwise processed in India;
- Incorporated or created under Indian law;
- Processing of personal data outside India if processing is in connection with any business carried on in India;
- Process personal data for the purpose of systematically offering goods or services in India; or
- With any activity involving profiling data principals within India

Terminology

- Data fiduciary - any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data (Controller),
- Data Processor - any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary;
- Data Principal - natural person to whom the personal data referred to.
- Person - an individual, a Hindu undivided family, a company a firm, an association of persons or a body of individuals, whether incorporated or not, the State, and every artificial juridical person, not falling within any of the preceding

PAI

Personal Data

- Is data about or relating to a natural person directly or indirectly identifiable, regarding characteristics, traits, attributes or any other features of the identity of such natural person,
- Any combination of such features, or any combination of such features with any other information;
- Sensitive Personal Data is data revealing, relating to or constituting passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric, genetic, transgender status , intersex status, caste, tribe racial or ethnic origin, religious beliefs, political opinions, political opinion, data,
- Anonymized data is not considered personal data.

Legal Bases for Data Processing

- Done with the express consent of the data principal;
- Necessary for functions of Parliament or any State Legislature;
- Necessary for compliance with a law or order of court or tribunal
- Necessary for prompt action (e.g. medical emergencies)
- Necessary for employment related purposes
- Necessary for reasonable purposes (e.g. fraud prevention, whistle blowing, M&A, Infosec, credit scoring, debt recovery etc.)

PAI

General Principles of Data Protection

Processing must be done taking into consideration certain familiar general principles, such as:

- Lawful processing
- Purpose limitation
- Collection limitation
- Notice
- Data Quality
- Storage limitation
- Transparency and Accountability (e.g. PbD)

Data Principal Rights

Examples:

- Right of confirmation and access
- Right of correction
- Right to data portability
- Right to be forgotten

Breach Notification

- Must notify DPA if breach likely to cause harm as soon as possible after a data breach and not later than time specified by the DPA (not yet determined),
- DPA will determine whether the data subjects must be notified and what mitigating steps must be taken by the company.

International Data Transfers

- Data fiduciary must ensure the storage, on a server or data center located in India, of at least one serving copy of personal data to which PDPA applies.
- The Central Government will notify categories of personal data as critical personal data that shall only be processed in a server or data center located in India.

International Data Transfers

- Personal data other than those categories of sensitive personal data notified may be transferred outside the territory of India where the transfer is made:
- Subject to standard contractual clauses or intra-group schemes that have been approved by the Authority; or
- The Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible;
- The Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or
- The data principal has consented to such transfer of personal data;
- The data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data notified by the Central Government.

PAI

Data Protection Officers (DPOs)

DPO must be appointed by each data fiduciary to:

- Provide advice on compliance
- Monitor processing activities
- Advise on manner of conducting DPIAs
- Act as a communication channel between the data fiduciary and the data protection authority
- Act as point of contact for data principal regarding complaints
- Maintain inventory of all records maintained by data fiduciary

Required even if not in India

PAI

Data Protection Impact Assessments

- The PDPA requires companies to generate a data protection impact assessment (DPIA) before undertaking personal data processing involving new technology, large scale profiling, or use sensitive data which carries a significant harm to data principals
- The DPIA must document data processing activities that create risks to data principals, as well as the measures, safeguards and mitigation mechanisms the company has implemented to address those risks

PAI

Record-Keeping

Must maintain detailed records of:

- Important operations in the data life cycle
- Periodic review of security safeguards
- DPIAs
- Other records of processing as determined by the DPA

Audit

The data fiduciary must audit its policies and its conduct of processing annually by independent data auditor:

- clarity and effectiveness of notices;
- effectiveness of measures adopted under PbyD;
- transparency in relation to processing activities
- security safeguards;
- instances of personal data breach and response of the data fiduciary, including the promptness of notification to the DPA; and
- any other matter as the DPA may specify

PAI

Information Security Requirements

Based on the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data fiduciary and the data processor shall implement appropriate security safeguards including:

- use of methods such as de-identification and encryption;
- steps necessary to protect the integrity of personal data; and
- steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data.

Every data fiduciary and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly

Penalties

A ***crore*** (/krɔːr/; abbreviated **cr**) or ***koti*** denotes ten million (10,000,000 or 10^7 in scientific notation) and is equal to 100 *lakh* in the Indian numbering system as **1,00,00,000** with the local style of digit group separators (a *lakh* is equal to one hundred thousand and is written as 1,00,000).

Penalties

Up to five crore rupees or two per cent of its total worldwide turnover of the preceding financial year, whichever is higher for failure to meet its obligation to:

- take prompt and appropriate action in response to a data security breach
- undertake a data protection impact assessment by a significant data fiduciary
- conduct a data audit by a significant data fiduciary
- appoint a data protection officer (by a significant data fiduciary)
- failure to register with the Authority under sub-section (2) of section 38.

PAI

Penalties

Up to fifteen crore rupees or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher

- processing of personal data in violation of the provisions of data protection obligations or grounds for processing of personal data
- processing of sensitive personal data in violation of the provisions of grounds for processing of sensitive personal data
- processing of personal data of children in violation of the provisions of personal and sensitive personal data of children
- failure to adhere to security safeguards;
- transfer of personal data outside India in violation the conditions for cross-border transfer of personal data

PAI

Chinese Security Rules

Chinese Privacy Landscape

- No single Chinese Privacy Law
- Like the US, the rules are fragmented across multiple pieces of legislation issued by authorities at various levels and with various jurisdictions
- At the **national** level, the laws include:
  - The PRC Criminal Law prohibits sale or illegal provision of, or illegal access (such as theft) to citizens' personal information;
  - The Provisions on Telecommunication and Internet User Personal Information Protection (effective from September 1, 2013), which are applicable to telecom and Internet service providers;
  - The Guidelines for Data Governance of Banking Financial Institutions, which are applicable to banking financial institutions established within the territory of the PRC licensed by the PRC banking regulatory authorities;
  - The People's Bank of China's Circular on Further Intensifying Management of Credit Information Security (effective from May 2, 2018) setting out obligations to strengthen credit information security in relation to access to database for financial credit information;
  - The PRC Consumer Rights Protection Law (effective from March 15, 2014) (Consumer Protection Law) contains data protection obligations which are applicable to most if not all types of businesses that deals with consumers. The Consumer Protection Law was supplemented by the Measures on Penalties for Infringing Upon the Rights and Interests of Consumers (effective from March 15, 2015).
  - Further, the draft Implementation Regulations for the PRC Consumer Protection Law released on 5 August 2016 will, if implemented, reiterate and clarify some of the data protection obligations as regards consumers' personal information; and
  - The PRC E-Commerce Law (effective from January 1, 2019), reiterating requirements to protect personal information in an e-commerce context (E-commerce Law).

PAI

Chinese Privacy Landscape

- On June 1, 2017, the PRC Cybersecurity Law came into effect and became the first national-level law to address cybersecurity and data privacy protection
- Much effort to clarify the significant ambiguities
  - Draft Guidelines on Multi-Level Protection Scheme for Information Systems released on June 27, 2018;
  - Draft National Standard of Information Security Technology – Guidelines for Personal Information Security Impact Assessment released on June 11, 2018;
  - Draft National Standard of Information Security Technology – Guidelines on Data Security Capability Maturity Model released on September 29, 2018; and
  - Draft Guideline for Internet Personal Information Security Protection released on November 30, 2018.

PAI

Chinese Privacy Landscape

- In addition to the PRC Cybersecurity Law, the following (together with a number of new laws and regulations released and passed to supplement the PRC Cybersecurity Law) constitute the framework of general data protection rules:
  - The Decision on Strengthening Online Information Protection, effective from December 28, 2012 (Decision)
  - National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services, effective from February 1, 2013 (Guideline)
  - National Standard of Information Security Technology – Personal Information Security Specification, effective from May 1, 2018 (PIS Specification)

PAI

PRC Cybersecurity Law

- Consists of 79 articles in seven chapters
- Contains an overarching framework targeting the regulation of internet security, protection of private and sensitive information, and safeguards for national cyberspace sovereignty and security
- Applies to "network operators" and critical information infrastructure (CII) operators
  - "Network operator," as defined could be applicable to almost all businesses in China that own or administer their internal or external networks
  - CIIs include, but not limited to, communications, information services, energy, transportation, utility, financial services, public services and government services

PAI

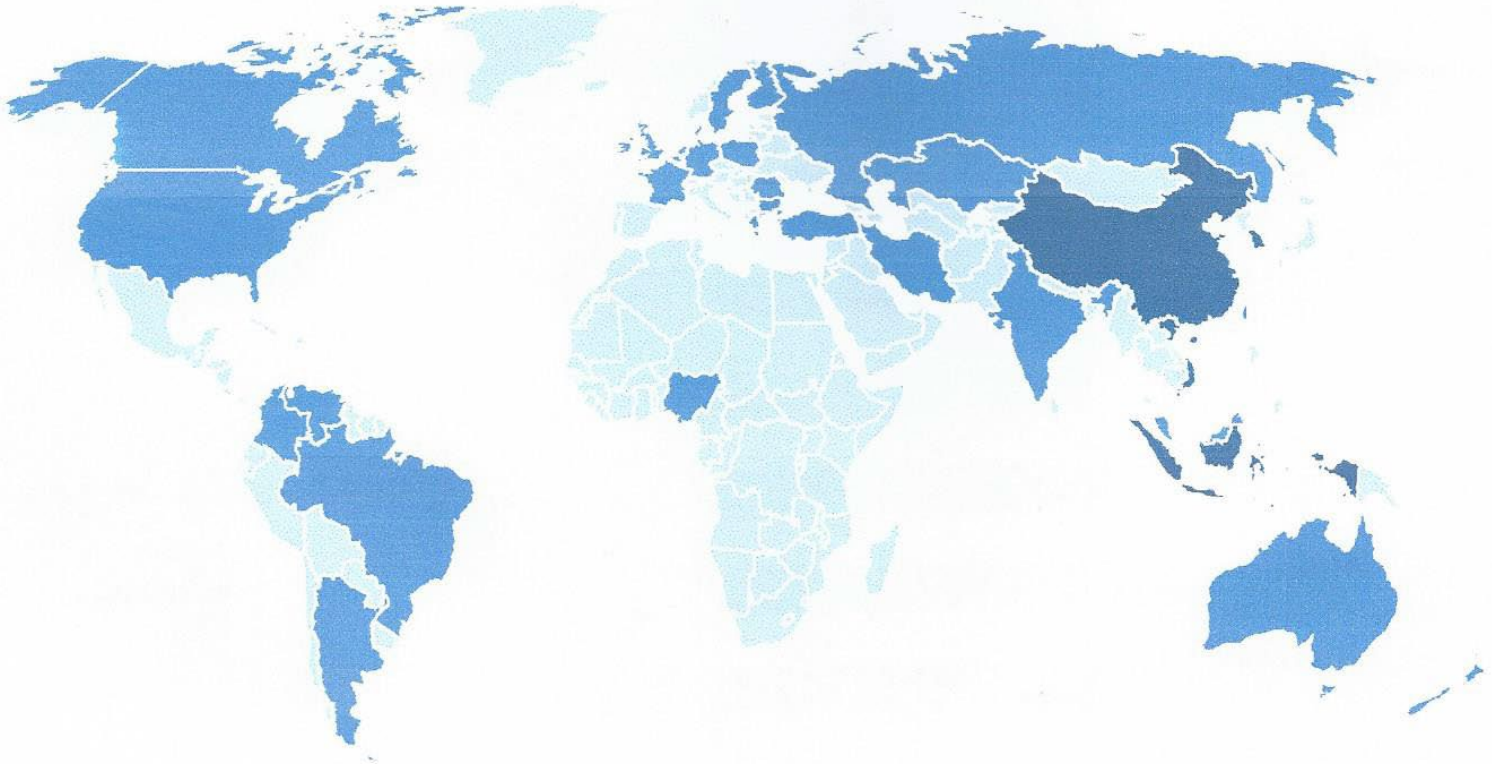
PRC Cybersecurity Law

- Different requirements for Network operators and CII operators
- Looks like a NIST or ISO standard, but with less specificity
- Penalties for violations include:
  - Monetary fines from RMB 5,000 to RMB 1,000,000
  - Suspension or termination of an enterprise's business license,
  - Removal of individuals from office
  - Criminal liability

Data Localization Law Metastasis

Blocking the Global Flow of Data

Which Countries Block Data Flows?*



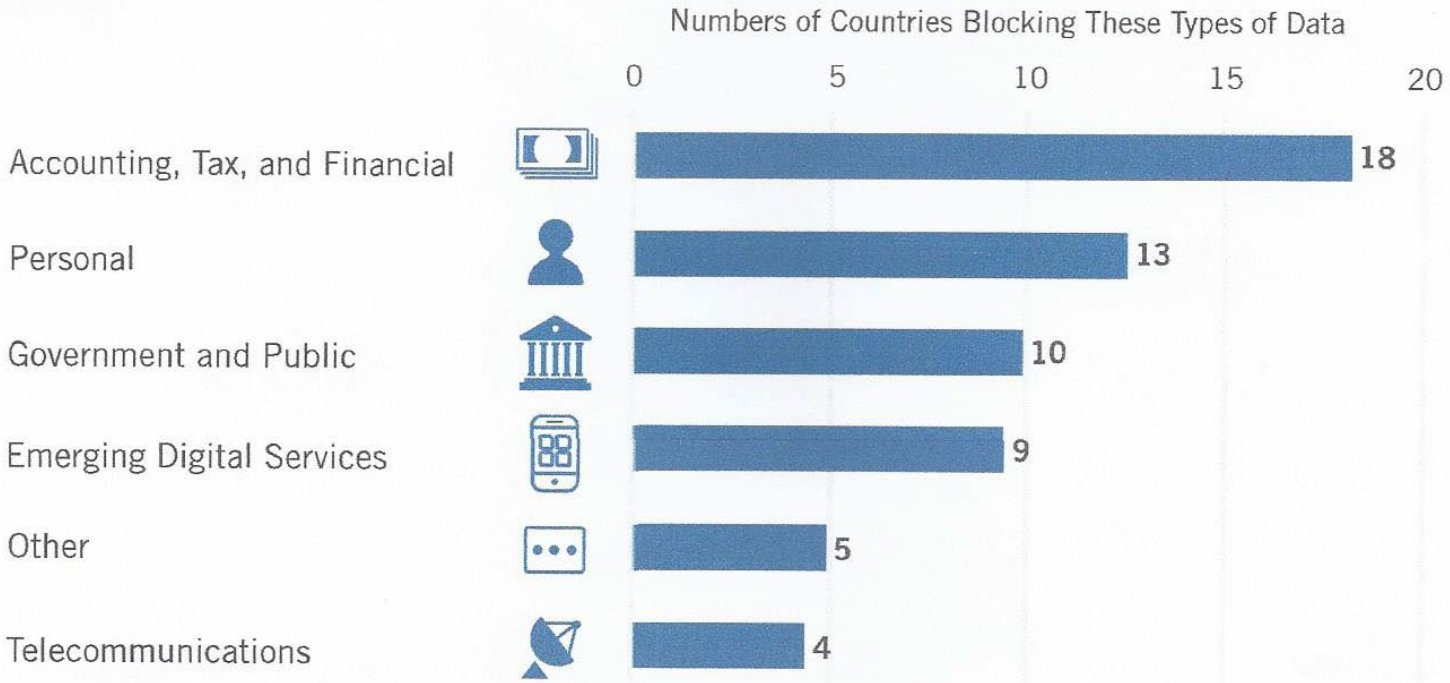
No data blocked

1-2 types of data blocked

3+ types of data blocked

PAI

What Types of Data Are Blocked?*



ITIF analysis of formal laws or regulations publicly reported as of April 2017.

Learn more at itif.org/databarriers

ITIF
INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

PAI