WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

WEBINAR

WilmerHale Cybersecurity, Privacy and Communications Webinar: Emerging Privacy and Cybersecurity Laws in Latin America and Asia

DECEMBER 6, 2018

Speakers: Reed Freeman and Nicole Ewart

Webinar Guidelines

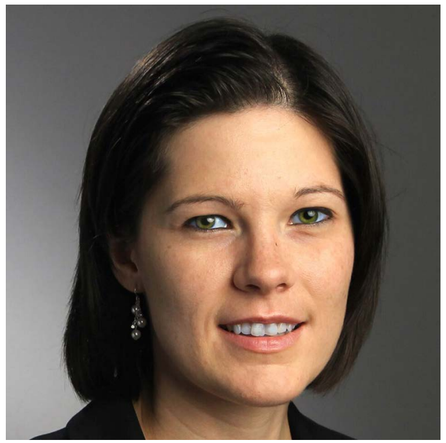
- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire program.

WEBINAR

Speakers

Reed Freeman
Partner
WilmerHale



Nicole Ewart
Senior Associate
WilmerHale

Agenda

- Emerging Laws in Latin America
- Emerging Laws in Asia
- Trends
- What’s on the Horizon

TOPIC

Emerging Laws in Latin America

Latin America

The EU Directive and now GDPR has influenced the laws in the region.

Common Characteristics

- In Latin America, unlike the European approach, there is a **heavy reliance on consent** to legitimize transfers to inadequate countries (and for collection generally).
- About half of the laws have **short data subject request response periods** of 10 days or less.
- A handful of laws protect personal information of both natural and legal persons.
- Many of the laws require registration.

Argentina

Personal Data Protection Act

- Based heavily on the EU Directive
- Express, **written consent** required to process personal data
- Transfers
  - Permitted where there is adequate protection, express consent, or another exception.
  - Model Clauses
- Moderate Enforcement

Draft Data Protection Bill

- Heavily based on the GDPR
- Would only apply to individuals
- Similar jurisdictional reach
- Allows for other bases for processing personal data beyond consent (such as “legitimate interest”)

Brazil

Personal Data Protection Law (enacted August 2018).

- The law will take effect in February 2020.
- Largely inspired by the GDPR

— Scope

- Applies to online and offline data.
- Extraterritorial reach

— Lawful Bases for Processing

- Expands bases for processing of personal data beyond the current consent regime.

— Data subject rights

— Data Protection Officer Requirements

Brazil, continued

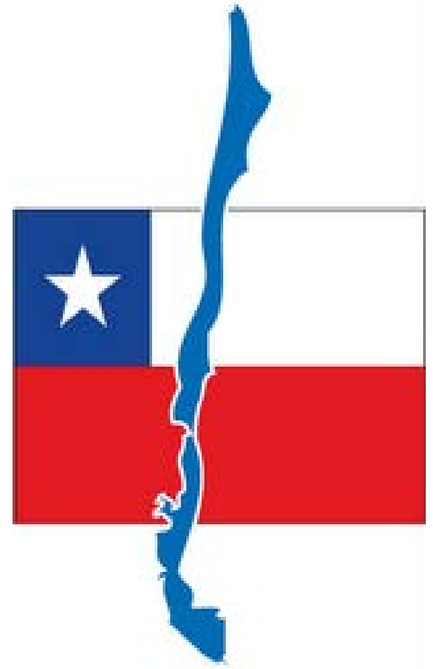
— Transfers

- Authorizes international data transfers provided participating countries have “adequate protection” for personal data.
- In absence of adequacy – standard contractual clauses or binding corporate rules, or with a specific and highlighted data subject consent

— Penalties

- Include: warnings, fines, publication of the condemnatory decision in newspapers
- Fines may reach up to 2% of gross revenue, limited to BRL 50 Million (appx. $13.5 million USD)
- **Enforcement in question:** The President vetoed a portion of the bill that would have created a body to regulate companies and verify compliance.

Chile



Law on Protection of Personal Data

- Does not restrict cross-border transfers
- No DPA to oversee enforcement
- A data subject's written consent is required for processing

Draft Bill – April 2018

- Currently being reviewed and processed in the Senate
- Consent remains the general rule for processing personal data, but the bill would establish new sources of lawfulness for processing data
- Expands data subject rights, similar to GDPR
- Imposes international transfer restrictions
- Creates a personal data protection agency

Constitutional Amendment

- June 2018 amendment to the Chilean constitution ensures the right to the protection of personal data

Mexico

Mexico's data protection law has a number of important differences from those found elsewhere in the region:

- Notice and data security obligations are subject to detailed rules.
- The law does not require registration, but it does require the appointment of a DPO and data security breach notification.
- Domestic and international transfers are largely subject to the same requirements.

Consent

- Required for all processing of personal data (with limited exceptions).

Data Subject Rights

- Right to access, amend, request deletion, or object to processing
- Controllers must respond within 20 days, unless an exemption applies.

Moderate Enforcement

Nicaragua

Law on Personal Data Protection

- One of the first laws to include the **right to be forgotten**
  - Applies to social networks, browsers, and servers
- Enforcement authority for the law has yet to be established
- Consent-heavy
- Database registration requirements
- International transfers of data may only be made to countries or organizations which provide adequate levels of security
  - And all transfers require consent of the data subject
- Controllers must respond within **10 days** to data subject requests

Peru

Law for Personal Data Protection

- Requires registration
- Breach notification requirements
- Data transfers
  - Cross-border transfers are permitted if the recipient country has adequate data protection, with some exceptions.
  - A 2017 amendment requires registering international data transfers in the National Registry for Personal Data Protection
- Prior, informed, express, and unequivocal consent is generally required for the processing of personal data, with some exceptions.
- Data subject access, correction, and deletion rights, and right to be forgotten
  - Must respond to access requests in 20 days, and other requests in 10 days
- Active enforcement with moderate fine amounts

Uruguay

Law on the Protection of Personal Data and Habeas Data Action

- Modeled after the EU Directive and deemed adequate by the EU

– Other features:

- Applies to individuals and legal entities
- No distinction between controllers and processors
- Database registration requirements
- Consent-heavy
  - With limited exception, must obtain **prior, express consent** from Data Owners before the data is collected and processed
- Access, correction, are deletion request responses must be made within **5 business days**

Other Latin American Countries

Colombia

- Law passed in 2012, similar terms to the EU Directive, but consent-heavy
- Parental consent required to process personal data of minors under 18
- Data controllers must register their databases (each database must be registered separately)

Costa Rica

- Based on the EU Directive
- Notice and express written or electronic consent requirements
- Data subject requests must be responded to within five working days
- Except for “internal databases,” all databases must be registered with the DPA

Panama

- Constitutional data protection provisions
- **Draft Data Protection Legislation**

TOPIC

Emerging Laws in Asia

Emerging Laws in Asia

Many new and revised laws in Asia are adopting elements of the GDPR

- There is a greater demand for data protection in the region.
- Like Latin American countries, many of the laws in the region are consent-heavy.

— Data Transfer

- In July 2018 the EU and Japan entered a trade deal which also recognizes each other's data protection regimes as adequate.
- The EU and South Korea began talks at the end of October regarding a data transfer pact.
- EU-APEC data transfer pact discussions are also occurring.

China

Cybersecurity Law

- Applies to “network operators” and “key information infrastructure operators”
- Key Information Infrastructure Operators (and likely Network Operators) must keep personal information within China
  - Exceptions may apply, but the law is new and still unclear.
  - Transfers may be permitted if “necessary” for “business needs” after a security assessment.
- Network operators are required to establish information protection systems.
- Tiered system for cybersecurity protection

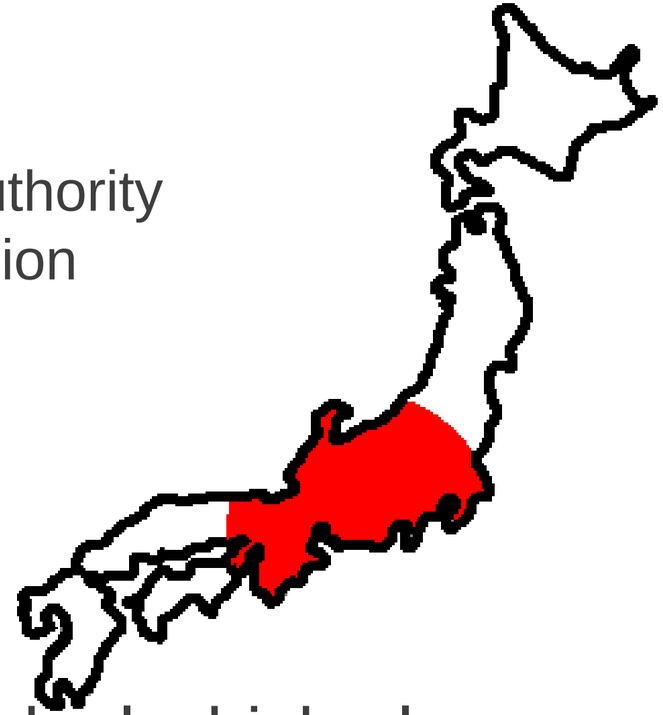
Personal Information Security Specification” (PI-Specification)

- Provides guidance on the collection, storage, use, transfer, and disclosure of personal information
- **Voluntary, not legally binding** (but expected to be taken under consideration by regulators when enforcing cybersecurity obligations)

Japan

Act on Protection of Personal Information

- Implemented in 2003 and amended in December 2016
  - Amendments consolidated the Data Protection Authority into the Personal Information Protection Commission
- Opt-in consent is required for:
  - Transfer of personal information to third parties (other than processors)
  - Transfer of information out of Japan
  - To send electronic marketing



In July 2018 the EU and Japan entered a trade deal which also recognizes each other's data protection regimes as adequate.

South Korea

Personal Information Protection Act and IT Network Act

- Data protection officers are required under PIPA, and a Director or Chief Officer must be designated under the IT Network Act.
- No distinction between controllers and processors
- Consent-heavy
  - Opt-in consent is generally required to transfer data to a third party.
  - Separate consents are required for each processing activity – collection, transfer, transfer outside of South Korea, sensitive data.
- Data subjects have rights to access (i.e., receive) information on, correct, delete, and suspend the processing of their personal information.
- Data subject notice and privacy policy are separate requirements.
- Active and strict enforcement of the laws

Collection and use of location information is heavily regulated under a separate law.

Vietnam

Cybersecurity Law (effective Jan. 1 2019)

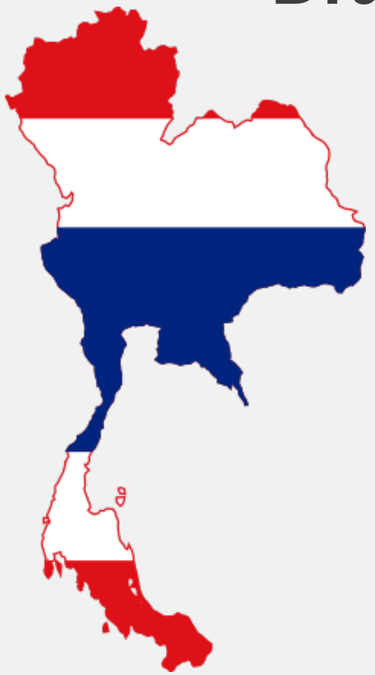
- Operators of Information Systems Critical to National Security (“CIS”) will have **data localization** and other broad obligations.
- Foreign companies providing telecommunications or internet services in Vietnam must:
  - Establish offices in Vietnam
  - Store the personal information of Vietnamese users and “other important data” in Vietnam and perform a security assessment prior to any cross-border data transfer; and
  - Bring their technology products involving cyber services into compliance with "quality assurance" standards before they can be released to the market.
- Companies will also be required to share data with the government if a user is suspected of anti-state activity.

Thailand

Thailand has a consent-heavy data protection regime

- Prior **written consent** is required for transfers to third parties.

Draft Data Protection Bill



- Adopts some provisions from the GDPR, including extraterritorial applicability
- Requests for consent from a data subject must be made explicitly for the consent given to be valid.
- Other lawful bases are adopted to process personal data
  - Thailand is one of the few jurisdictions in the region to introduce the concept of a data controller's "legitimate interest" as a basis for processing beyond consent.
- Similar data subject rights as in the GDPR, including portability

Malaysia

Personal Data Protection Act

- Data Users must obtain consent before any personal data may be collected or processed, with limited exceptions.
- Access, correction, and deletion rights for data subjects
- Transfers
  - Permitted to countries with adequate data protection laws
  - Or with data subject consent
  - Transfers of data through cloud computing services are not permitted without the written consent of an officer authorized by top management.
- **Malaysian Personal Data Protection Commissioner is currently considering a data breach notification requirement (72 hours)**

Singapore

Singapore's Cybersecurity Bill (passed February 5, 2018)

- Regulates providers of Critical Information Infrastructure
- Does not apply to multinationals with Singapore offices supported by infrastructure located overseas
- Calls for the appointment of a Cyber Security Commissioner with broad powers extending beyond CIIs
- Creates a framework for licensing and regulating service providers of certain types of cybersecurity services (includes overseas service providers)

Personal Data Protection Act

- Consent is the general rule.
- An organization must ensure "comparable protection" to the standards set out in the Act when transferring personal data outside of Singapore.
- The Personal Data Protection Commission is considering significant changes to the existing framework re: breach notification and consent.
- Moderate and increasing enforcement levels

India

The Supreme Court of India declared privacy a fundamental right in August 2017.

Personal Data Protection Bill, 2018

- Submitted to the Ministry of Electronics and Information Technology in July 2018.
- Data principals (subjects) are granted a number of rights, such as access, correction, data portability and the right to be forgotten
- Requires annual data audits by third parties
- GDPR-type extraterritoriality and penalties
- **Data Localization:** requires storage of a copy of personal data in India and “critical personal data” can *only* be stored in India
- Data transfer restrictions

Indonesia

Gov. Reg. 82 and MCI Regulation 20/2016

- Applies to Electronic System Providers
- Data subjects must be given notice (in the Indonesian language), and **written consent** is generally required for any use of personal data.
- Personal data can be transferred to a third party processor with consent.
- Data subjects generally have the right to access, correct, or delete their data.
- Data can be transferred out of Indonesia after coordination with the Ministry of Communication and Informatics and either with consent of the data subject or where the subject has been informed and steps have been taken to safeguard the data.
- **Localization:**
  - ESPs that provide public services must store data locally and register with the authority.
  - **Some sector-specific localization requirements**

Other Laws

Taiwan

- Moderate enforcement mostly around data breaches
- No centralized authority; a variety of governmental agencies can enforce.

Hong Kong

- One of the region's best developed data protection laws, with the Personal Data (Privacy) Ordinance dating back to 1995
- The PCPD has stated that it is closely monitoring the implementation of the GDPR.

Philippines

- Enacted in 2012, but the enforcement authority was not created until 2016
- Some GDPR elements in implementing rules and regulations, such as 72 hour data breach notification requirement, and data portability

APEC Cross-Border Privacy Rules

The APEC Cross-Border Privacy Rules ("APEC CBPR") system was endorsed in 2011

- A voluntary, principles based privacy code of conduct for data controllers in participating APEC member economies
- Relates only to cross-border data flows

— Increasing participation

- Last year **Australia** announced its intention to become the sixth country to participate in the system (alongside Canada, Japan, Mexico, United States, and South Korea).
- **Philippines**, **Singapore**, and **Taiwan** have announced intention to participate.

The APEC Electronic Commerce Steering Group (the "ESGC") met with the European Commission to begin discussions on recognizing the CBPR System as a certification under Article 42 of the GDPR.

TOPIC

Trends

Trends in Emerging Laws

- GDPR-like laws and provisions
  - Data transfer restrictions
  - Extraterritoriality
  - Expanded data subject rights, including portability
- Data breach notification requirements
  - Some 72-hour provisions
- Data localization requirements
- More significant penalties for violations and more active enforcement

TOPIC

What's on the Horizon

What's Coming?

More Laws

More Amendments

More Regulations

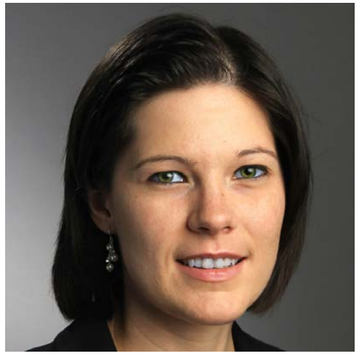
More Localization

More Compliance Concerns!

Questions?

Questions?

D. Reed Freeman
Partner
WilmerHale
Reed.Freeman@wilmerhale.com
+1 202 663 6267



Nicole Ewart
Senior Associate
WilmerHale
Nicole.Ewart@wilmerhale.com
+1 202 663 6692