OVERVIEW OF THE EVOLVING PRIVACY LANDSCAPE

Overview

1. Introduction to Data Privacy
2. Data Privacy Risks and Issues
3. Ways in which Data Privacy Laws Impact Information Governance
4. Recent and New Data Privacy Laws and Considerations

INTRODUCTION TO DATA PRIVACY

What is "personal information"

- Depends greatly on the law
- In most recent and emerging laws, it focuses (with some variation) on anything that can be used on its own or with other information to identify someone.
- May include personal information that is encrypted or otherwise not immediately accessible, e.g., employee ID numbers
- Sensitive personal information has multiple meanings as well and often carries heightened protection and treatment requirements

DIFFERENT STYLES OF PRIVACY LAWS

Comprehensive

- Example is the EU
- Covers all personal information (with perhaps small exceptions)

Sectoral

- Example is the US
- Is divided by purpose of the law, such as a healthcare or finance law

Co-Regulatory

- Example is Australia
- Federal law that allows industry regulations to be legally binding

DIFFERENT REASONS FOR PRIVACY LAWS

Protection of People	In some countries or regions, data protection is a fundamental human right or part of a constitution.
Concern for Both People and Business	While data privacy is important, some places balance concern for people with a desire to limit impediments on business
Economic Protection	• While data protection laws may provide for protections of individuals, underlying concerns may be protection of state interests and economy

DATA PRIVACY RISKS AND ISSUES


Your Vendors
Public Image
Your Entity
Your Client
Regulators

Client & Vendor Risks

Clients

- Clients have both commercial expectations and legal expectations which leads to a higher number of possibilities for violating these expectations
- Clients may be legally liable for your entity's actions
- Clients are pushing much harder lately for privacy elements in what used to be primarily security assessments and audits

Vendors

- You may be legally responsible for vendor's actions
- Transferring data to a vendor requires higher scrutiny for security and mandates trust (and therefore due diligence) in their ability to comply
- Possibility of international transfer may be increased

Regulator and Public Image Risks

For very different reasons the impact on business can be quite similar

- Regulators can often issue financial penalties, whereas the public (either individuals or other entities) can have a strong financial impact by discontinuing use of a business they know to violate data privacy requirements/laws
- Each can trigger the other:
  - Regulators investigating can cause the public to know and react
  - Outcry from the public can lead to regulatory investigation

WAYS DATA PRIVACY LAWS IMPACT INFORMATION GOVERNANCE

Records Management

- Necessity to be able to delete data creates complex needs in often antiquated systems
- Cross-border movement is both easy and often unknown unless practices are in place to notify certain teams
- Definition of a "record" may not align with "personal information" requiring either an update or divergent programs

Data Mapping/Movement

- Regular business processes create a multitude of locations where personal information ends up and travels through
- Third parties are commonly involved in many different service provisions
- Layered systems and practice can add complexity to creating a clean knowledge of where personal information goes

Interconnectivity of often siloed lines of business or corporate functions

- Information governance addresses a multitude of different data concerns, and without an intention to do so there may be walls between these teams and divisions with limited visibility into the others
- Intentional practices and crossover working groups can address these situations, as can a strong attention to Privacy by Design
- In many companies political issues may require particular finesse to integrate data privacy into functions and to push collaboration to minimalize risk

RECENT AND NEW DATA PRIVACY LAWS

International Data Privacy Laws

GDPR

Extraterritorial Scope

Strong penalty structure

Impacts nearly all personal information in EU

China Cybersecurity Law

- First law addressing privacy in China
- Includes still undefined data localization elements

Brazilian Data Protection Regulation (LGPD)

- Goes into effect in 2020
- Mirrors GDPR in most ways

Indian Data Privacy Act

- Still in draft form
- Mandated as privacy has been identified as a fundamental right

Where does the US fit in with data privacy?

- Current approach is very divided between many different federal, state, and local laws
- Country is very accustomed to inconsistent laws due to 50 different state-based breach reporting laws
- California Consumer Privacy Act (CCPA) goes into effect in-part January 1, 2020 and the remainder is slated to be in effect by July 1, 2020
- At current count 15 states aside from California have data privacy laws at some point in the legislative process
- These laws diverge greatly in their make-up
- This has increased discussion on a federal data privacy laws

Key Aspects of CCPA

- Scope – both territorial and entity
- Definition of personal Information
- Requirements for notice
- Verified Consumer Requests
- Opt-In and Opt-Out Requirements Depending on age
- Contractual Terms
- Requirements to provide equal service regardless of exercising of data rights
- Individual Cause of Action
- Attorney General Enforcement

DISCUSSION AND QUESTIONS

LAUREN KITCES

LAUREN.KITCES@WILLISTOWERSWATSON.COM