ACC Association of Corporate Counsel
WESTCHESTER/ SOUTHERN CONNECTICUT
(formerly WESFACCA)

Data Privacy in 2021 and Beyond

A Two-Part Analysis and Discussion

BARTON
Discover Better Law

KJ | Kennedy Jenks

mastercard.

SOMPO INTERNATIONAL

SPEAKERS:

Kenneth Rashbaum, Partner — Barton LLP
Gerard P. Cavaluzzi, EVP, General Counsel and Secretary — Kennedy Jenks
Elise Houlik, SVP, Assistant General Counsel, Privacy and Data Protection — Mastercard
Yukiko Lorenzo, Assistant General Counsel, Privacy and Data Protection — Mastercard (London)
Brian Leonardi, Assistant Vice President, Legal and Compliance — Sompo International

AGENDA

December 1, 2021

10:30 to 10:35 AM

- Introduction

10:35 to 11:10 AM

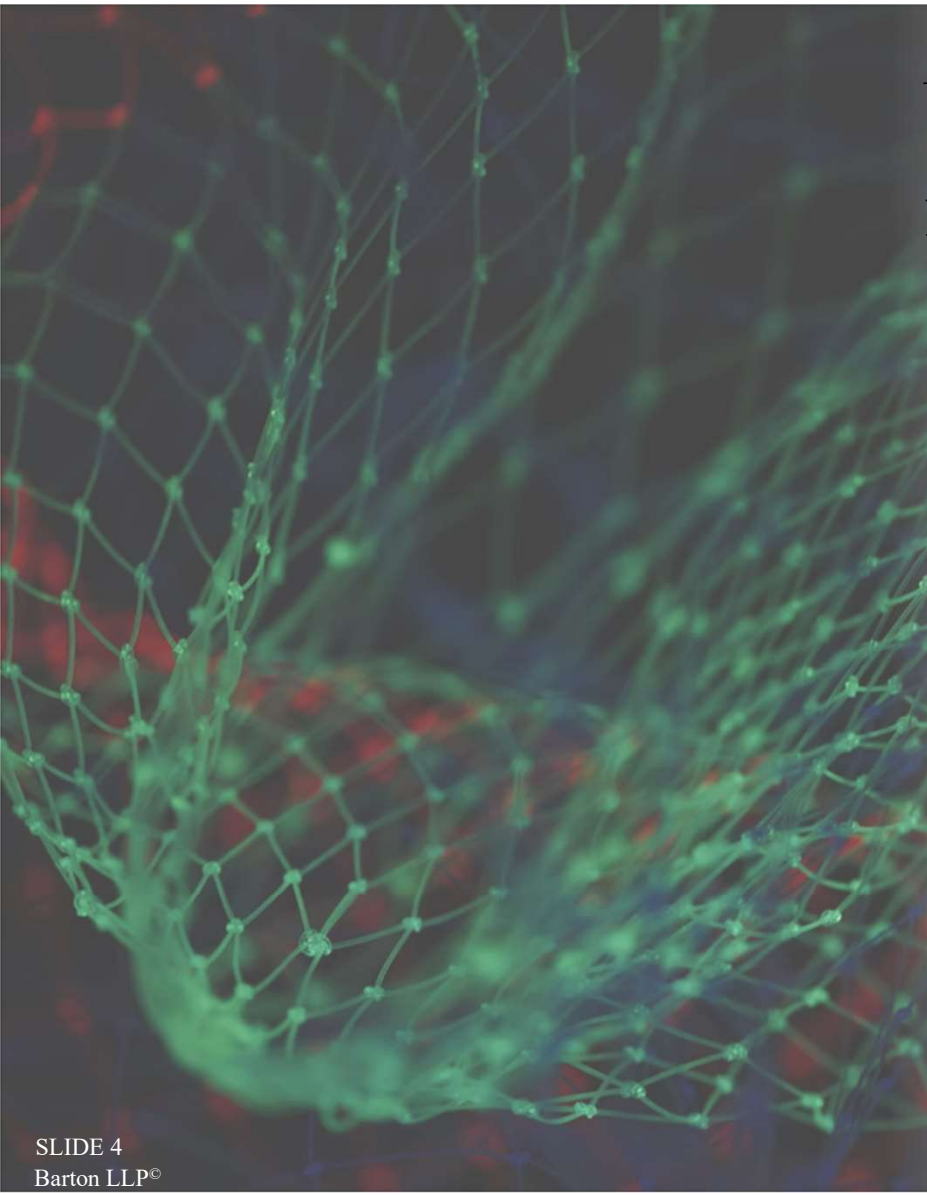
- Overview of US federal and state Laws: In effect, due to take effect and proposed

11:10 to 12:00 PM

- European Union, Asia and Beyond
  - The United Kingdom
  - Canada
  - Brazil

U.S. Federal Law: Sectoral Statutory Approach

- HIPAA (Healthcare)
- Gramm-Leach-Bliley Act (Financial)
- FERPA (Education)
- COPPA (Information regarding children)
- SEC Reg. S-P(Public Companies)

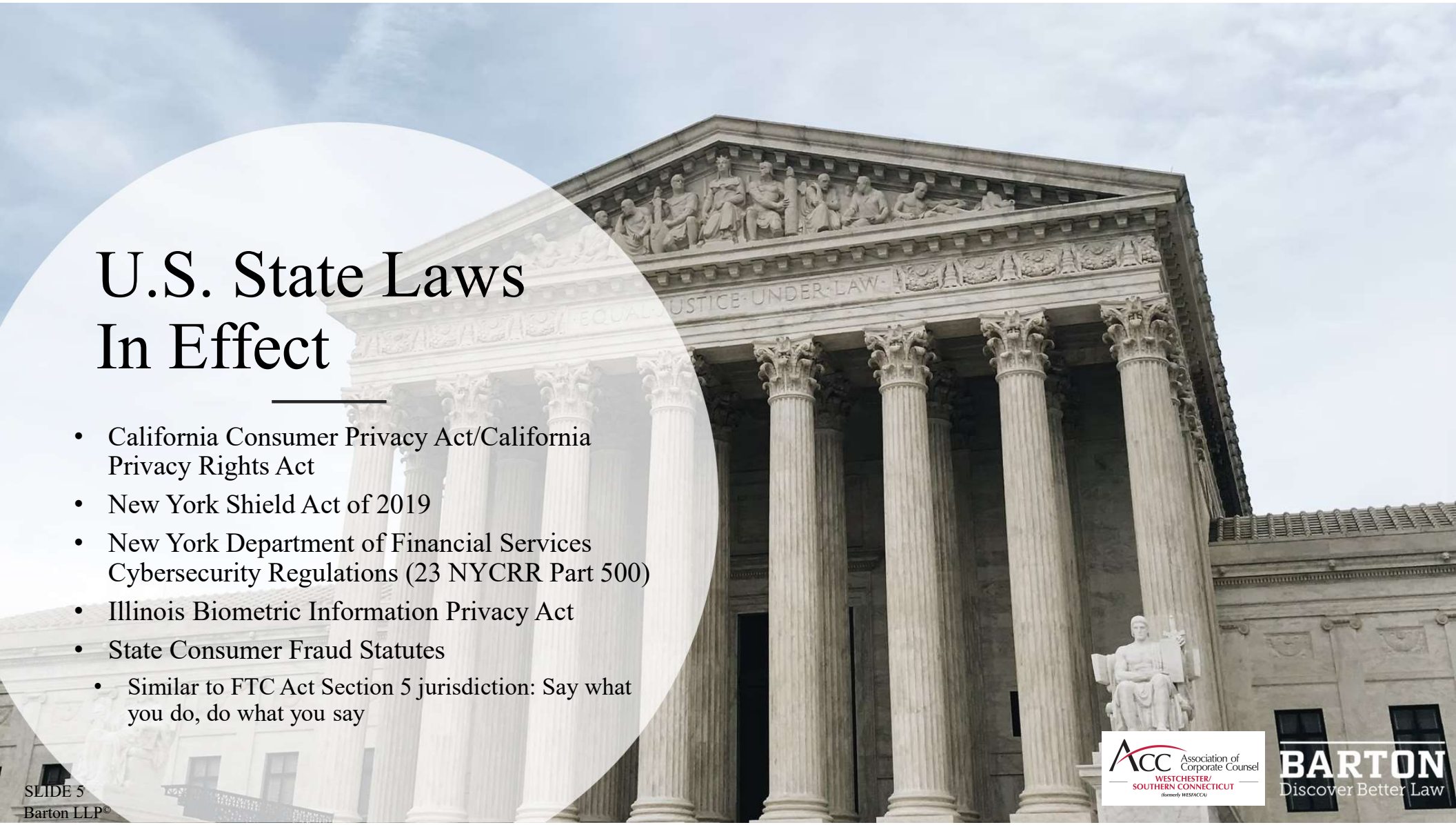


U.S. Government Agencies in Data Protection

- Office of Civil Rights of U.S. Department of Health and Human Services
- Federal Trade Commission
  - Section 5 Jurisdiction and Proceedings
- Departments of Justice and Commerce
  - Merger and Acquisition Review Approval
  - Executive Order 13873 ("Protecting Americans' Sensitive Data From Foreign Adversaries," June 9, 2021
  - "Executive Order On Promoting Competition in the American Economy," July 9, 2021
    - Data Protection considerations in FTC merger review
    - DOJ review includes anticompetitive collection and uses of personal data

ACC Association of Corporate Counsel WESTCHESTER/ SOUTHERN CONNECTICUT (formerly WESPACCA)

BARTON Discover Better Law

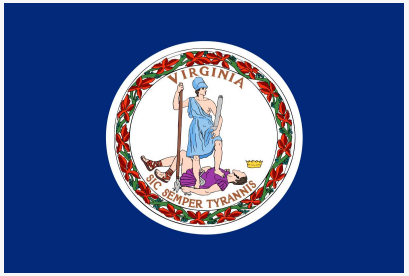


U.S. State Laws In Effect

- California Consumer Privacy Act/California Privacy Rights Act
- New York Shield Act of 2019
- New York Department of Financial Services Cybersecurity Regulations (23 NYCRR Part 500)
- Illinois Biometric Information Privacy Act
- State Consumer Fraud Statutes
  - Similar to FTC Act Section 5 jurisdiction: Say what you do, do what you say

U.S. State Laws Taking Effect in 2023 and In Process

- Virginia Consumer Data Protection Act (January 1, 2023)
- Colorado Privacy Act (July 1, 2023)
- In Process:
  - New Jersey
  - Washington State
  - New Mexico
  - Others in very preliminary stages



The Virginia Consumer Data Protection Act (VCDPA)

1

Second state to adopt a privacy law that grants its residents **privacy protections** and **control** over their personal data

2

Closely **aligns** with **GDPR** and **CCPA**, and creates **new requirements** for the handling of **sensitive data** types including biometrics, precise geolocation, and health information

3

Grants individuals the **right to access, correct, delete, and port** their personal data, along with the **right to opt-out** of behavioral advertising and certain data sharing, and **opt-in** to processing of their **sensitive personal data**

4

Data protection assessments required for targeted advertising, profiling, sensitive data processing, and activities that present a heightened **risk of harm to consumer**

5

Exemptions for **entities governed by GLBA**; and that use information for **fraud/security-related purposes**

6

Effective **January 1, 2023**. Fines can include up to **$7,500 per violation** if an organization does not **cure** a potential violation within **30 days** (no private right of action)

The Colorado Privacy Act (CPA)

1

On July 7, 2021, Colorado became the **third state** in the United States – and the **second in 2021** – to pass omnibus privacy legislation focused on **consumer privacy rights**

2

Obligations are **consistent** with those imposed in **California** and **Virginia**, but they are not identical, further adding to the fragmented approach to governing privacy rights in the United States, and globally

3

Grants individuals the **right to access, correct, delete, and port** their personal data, along with the right to **opt-out** of behavioral advertising and **opt-in** for **sensitive personal data processing**

4

Definition of **consent** move closer to **GDPR-like standards** by requiring an affirmative, specific act of choice and not derived from acceptance of general terms or a privacy notice

5

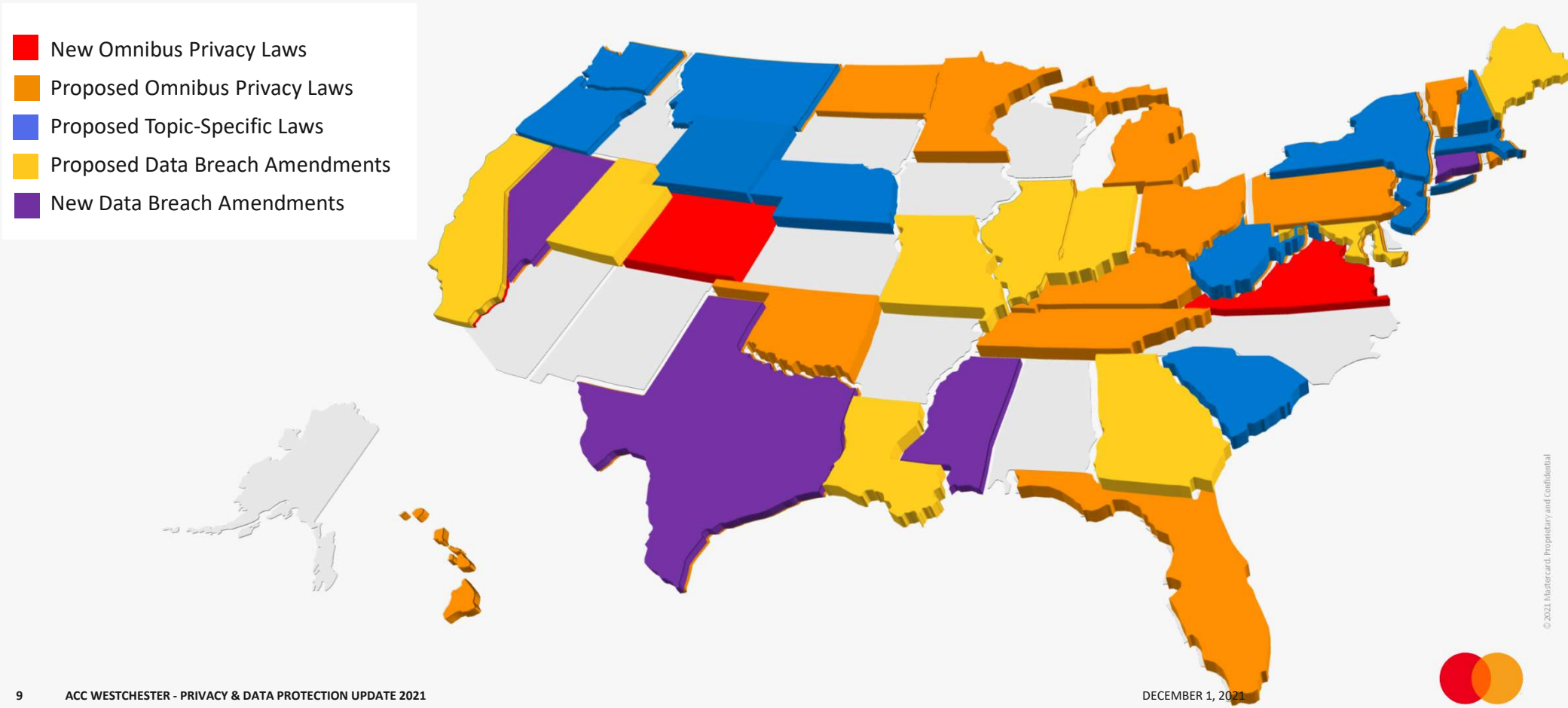
Prohibits dark pattern consent where consent is obtained through deceptive user interfaces that impair one's ability to make choices about how their information is processed

6

Effective **July 1, 2023**. Fines can include up to **$25,000 per violation** with a cure provision that will sunset in 2025 (no private right of action)

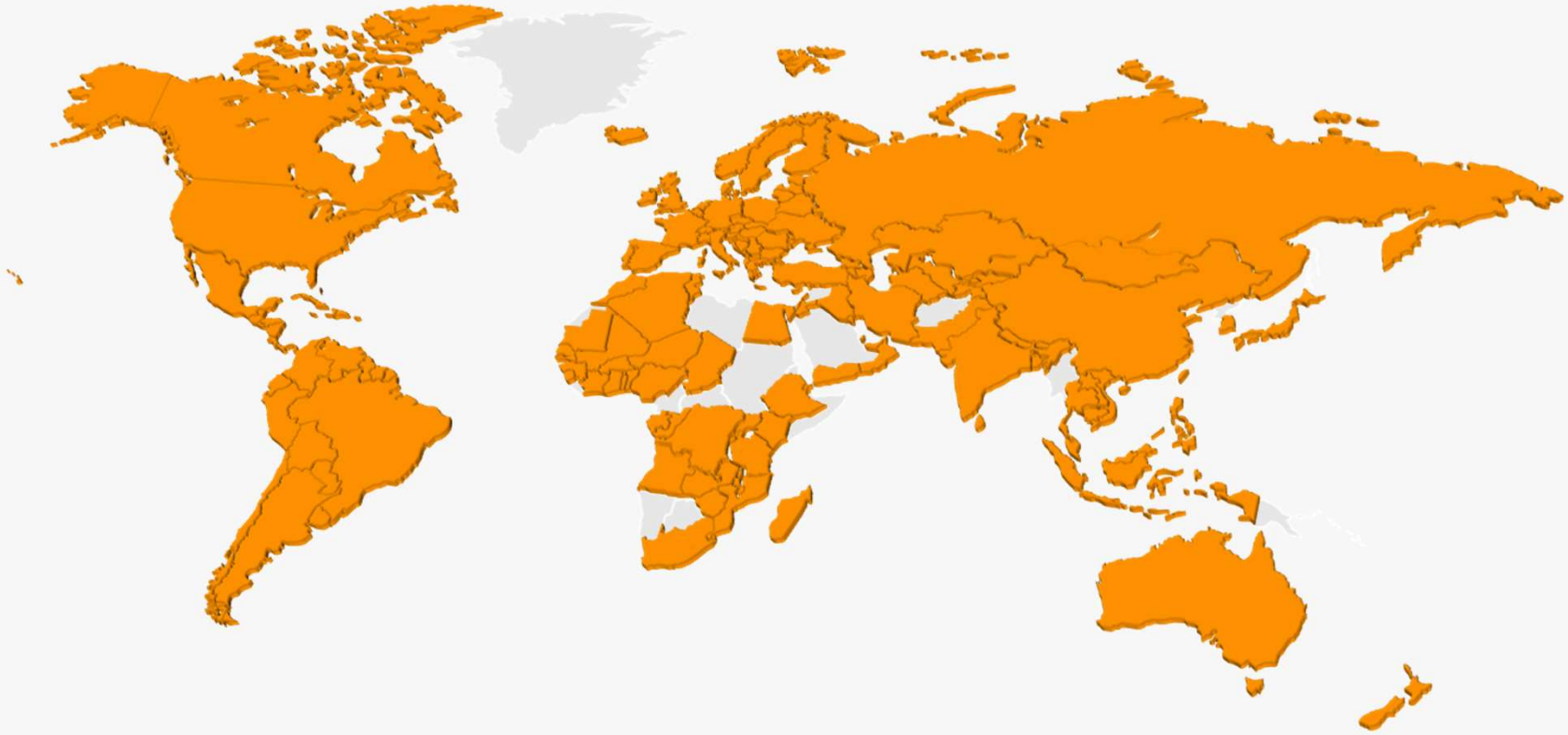
Privacy & Data Protection Laws

U.S. Developments for 2021 (for now….)



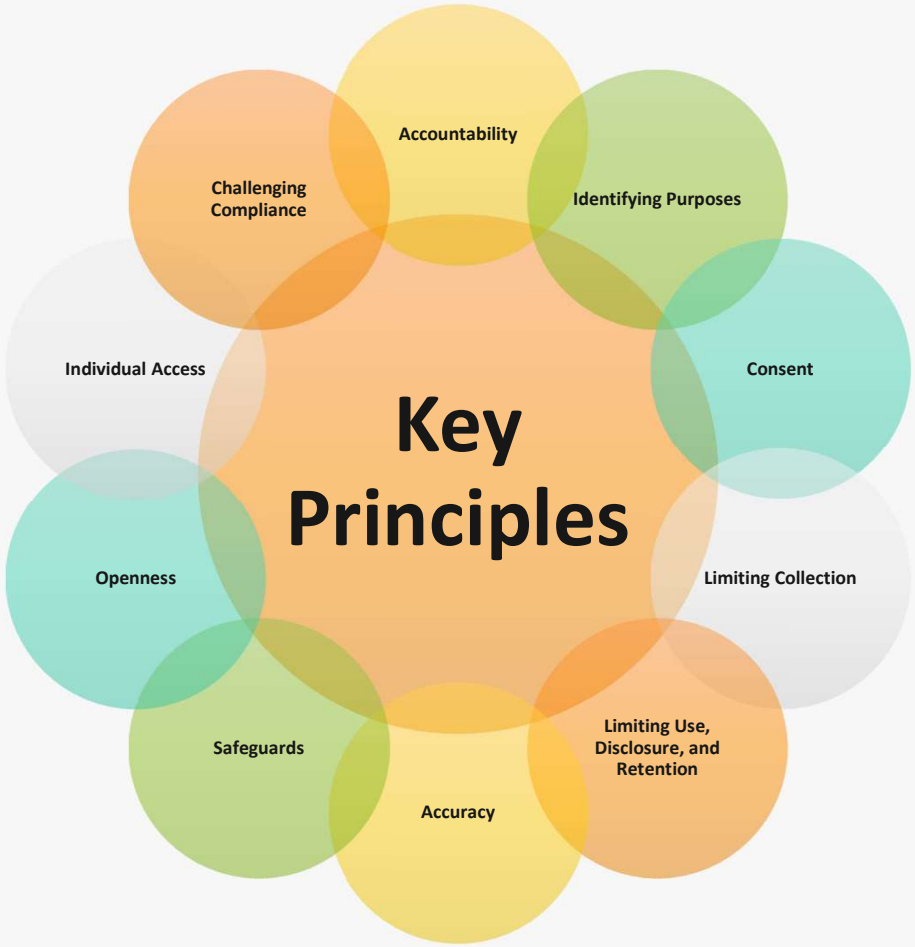
Privacy & Data Protection Laws

Data Protection Activity Across the Globe



Privacy & Data Protection Laws

Personal Information Protection and Electronic Documents Act (PIPEDA)



Quebec “Bill 64”

1

On September 21, 2021, Québec amended its existing privacy law to bring its terms more **in line with the standards set forth in the GDPR**

2

Obligations are **consistent** with those imposed in **PIPEDA,** but they are not identical, and additional governance requirements will be added for this province

3

Grants individuals the **right to access, correct, and port** their personal data, along with requirements around **automated decision-making** and **express opt-in** for **sensitive personal data processing**

4

There is an emphasis on analyzing the impact of **sending personal data outside of Québec** and addressing whether it will be adequately protected outside the province

5

With a staggered schedule, most requirements will become **effective on September 22, 2023**

6

Embedded administrative fines and penal penalties, along with a private right to action included for violation of several of the law’s provisions. Enforcement by the Privacy Regulator begins **September 22, 2023**

European Union

- *Schrems II* CJEU judgment and subsequent European Data Protection Board's Recommendations
  - Enforcement actions that led to suspension of EU personal data transfer to the US
- Sensitivity with the use of non-EU based cloud platforms
- EU data transfer impact assessments
  - New EU Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs)
- UK – adequacy decisions, UK SCCs and UK transfer impact assessment

GDPR Benchmark Assessment

Country	Scope		Definition & Legal Basis				Data Subject Rights					Enforcement		
	Personal	Territorial	Personal Data	Pseudony-mization	Controller & Processor	Legal Basis	Deletion	Informed	Object	Access	Portability	Supervisory Authority	Monetary Penalties	Civil Remedies
Brazil - LGPD														
China - PIPL														
Mexico - FLPP														

Inconsistent | Fairly Inconsistent | Fairly Consistent | Consistent

- The evolution of comprehensive privacy frameworks is evident when benchmarking other national privacy regimes against GDPR
  - Mexico's FLPP, which came into effect in July 2010, shares some similarities with GDPR (e.g. definition of PII, providing certain data subject rights, etc.); however, it is less robust in several key areas, including the FLPP's scope, rules regarding pseudonymization, defining processor/controller roles, and establishing legal basis for processing.
  - Laws passed more recently, including Brazil's LGPD (September 2020) and China's PIPL (November 2021) are generally consistent with the approach taken by GDPR (e.g. scope, defined terms, legal basis for processing, data subject rights, and enforcement).
- For organizations operating globally, the integration of GDPR considerations, including data privacy impact assessments and information security assessments, can help identify tent-pole data protection issues during due diligence, change management, etc.
  - Nonetheless, it is important that Legal & Compliance teams be involved early and often to ensure that adequate time is allotted to assess the applicable laws and regulations within each jurisdiction.
  - While most privacy laws passed within the past 3+ years share a great deal of similarity, key differences (e.g. consent, data transfer/localization, data security, etc.) may arise that create operational challenges and give rise to regulatory compliance risks.

ACC Association of Corporate Counsel
WESTCHESTER/ SOUTHERN CONNECTICUT
(formerly WESFACCA)

BARTON
Discover Better Law

KJ | Kennedy Jenks

mastercard.

SOMPO INTERNATIONAL