



*presents*

## **Inaugural Annual Privacy Law Summit**

Session 4

Keeping Pace With Privacy: Best Practices for Building A Multi-Jurisdictional  
Compliance Program

MCLE: 1.0 Hours

Thursday, February 9, 2023

3:15 p.m. – 4:15 p.m.

Speakers:

Steve Millendorf, Partner, Privacy, Cybersecurity, and Technology Practice Group,  
Foley & Lardner LLP

Chris Ghazarian, General Counsel, Dreamhost

Tami Dokken, Chief Data Privacy Officer, World Bank

Dona J. Fraser, Senior Vice President, Privacy Initiatives  
BBB National Programs

Conference Reference Materials

Points of view or opinions expressed in these pages are those of the speaker(s) and/or author(s). They have not been adopted or endorsed by the California Lawyers Association and do not constitute the official position or policy of the California Lawyers Association. Nothing contained herein is intended to address any specific legal inquiry, nor is it a substitute for independent legal research to original sources or obtaining separate legal advice regarding specific legal situations.

© 2023 California Lawyers Association

*All Rights Reserved*

PRIVACY  
LAW

CALIFORNIA  
LAWYERS  
ASSOCIATION

# Keeping Pace with Privacy - Best Practices for Building a Multi-jurisdictional Compliance Program

Inaugural Privacy Law Summit, Los Angeles, CA

Stephen Millendorf, Foley & Lardner,  
Tami Dokken  
Christian Hammerl (Moderator)

Chris Ghazarian, Dreamhost  
Dona J. Fraser, BBB

February 9 , 2023

# Keeping Pace with Privacy

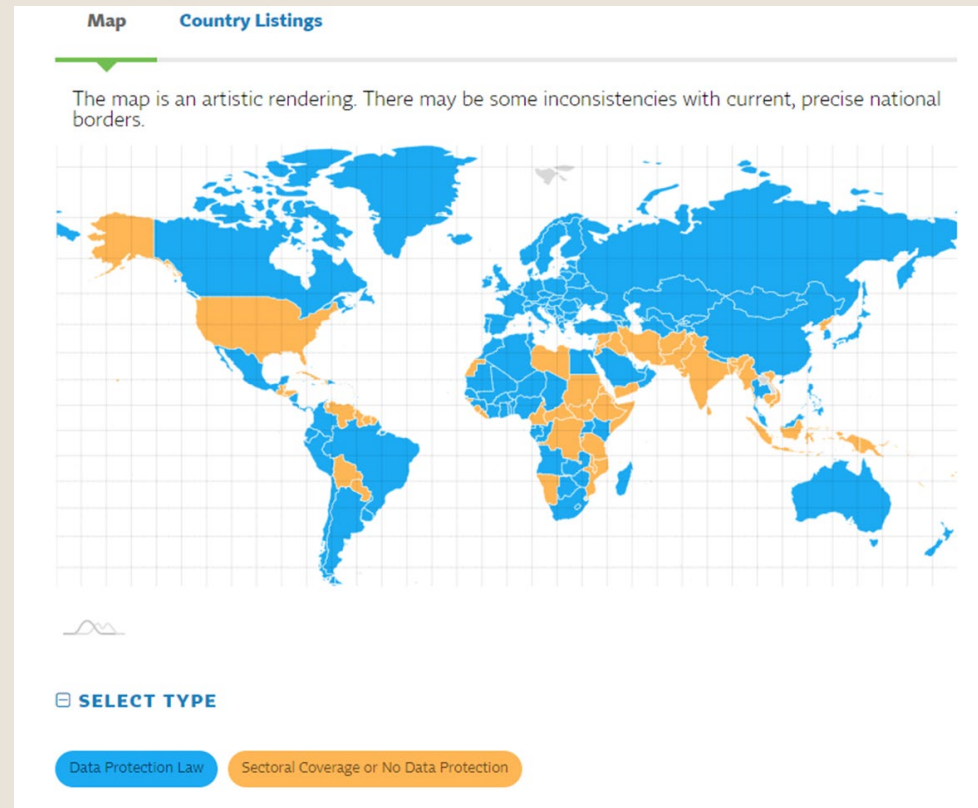
## Overview

---

- **Introduction**
- **Proliferation of Privacy Laws**
  - Expanding Compliance Obligations - Resource Constraints
- **Archetypes of Privacy Compliance Models**
  - ✓ Race to the Top
  - ✓ Policy-based Compliance (Approximation)
  - ✓ Selective Compliance
- **Key Components of Successful Compliance Strategies**

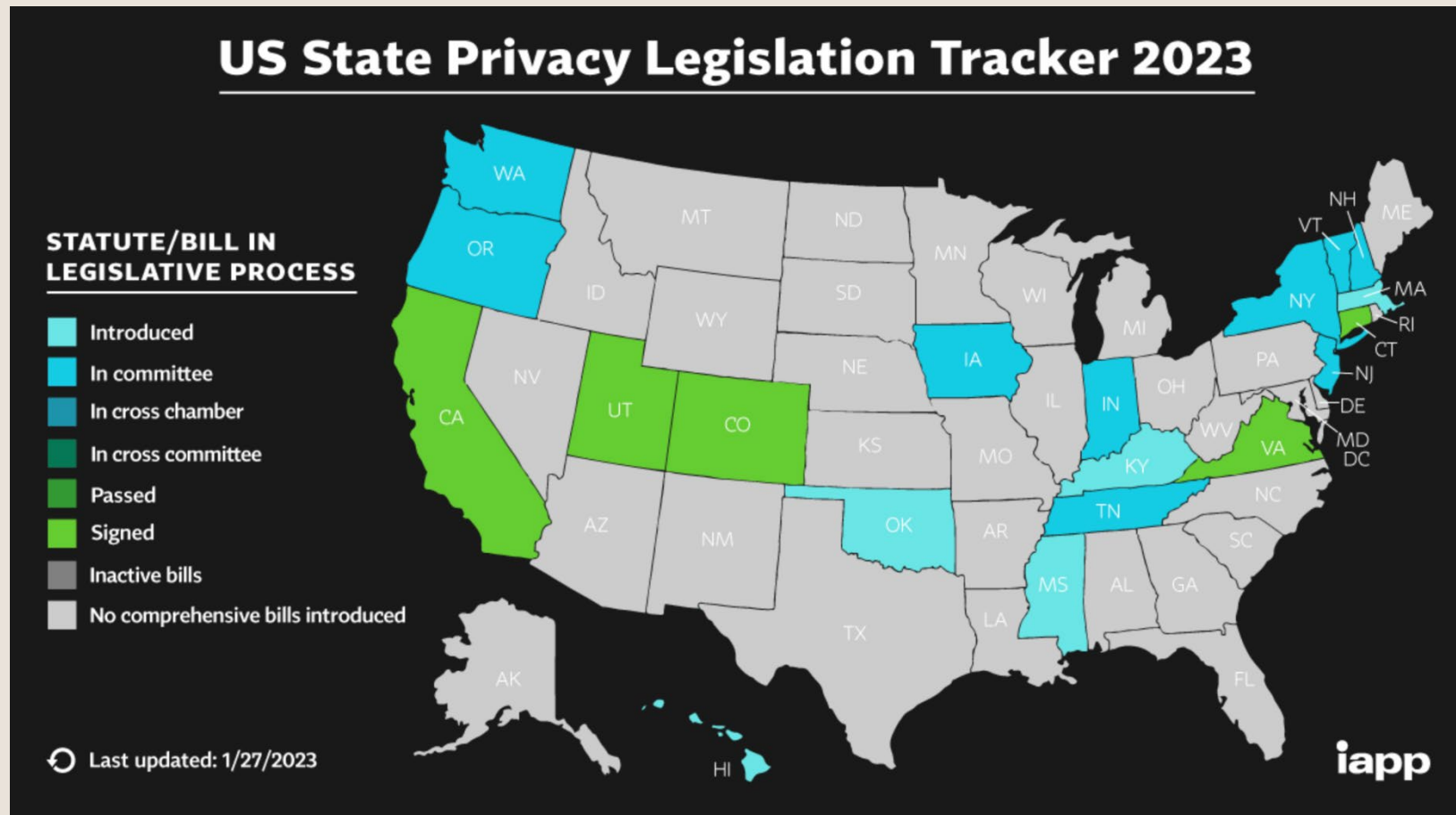
# Keeping Pace with Privacy

## Proliferation of Privacy Laws



# Keeping Pace with Privacy

## Proliferation of Privacy Laws



# Keeping Pace with Privacy

## Proliferation of State Privacy Laws

### State Privacy Laws in Force

<b>California</b>	<a href="#">CCPA</a>	California Consumer Privacy Act (2018; effective Jan. 1, 2020)
	<a href="#">Prop 24</a>	California Privacy Rights Act (2020; fully operative Jan. 1, 2023)
<b>Colorado</b>	<a href="#">SB 190</a>	Colorado Privacy Act (2021; effective July 1, 2023)
<b>Connecticut</b>	<a href="#">SB 6</a>	Connecticut Data Privacy Act (2022; effective July 1, 2023)
<b>Virginia</b>	<a href="#">SB 1392</a>	Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023)
<b>Utah</b>	<a href="#">SB 227</a>	Utah Consumer Privacy Act (2022; effective Dec. 31, 2023)

### State Privacy Laws Proposed

Hawaii, Iowa, Indiana, Kentucky, Massachusetts, Mississippi, New Hampshire, New Jersey, New York, Oklahoma, Oregon, Tennessee, Vermont, Washington

PRIVACY  
LAW

CALIFORNIA  
LAWYERS  
ASSOCIATION

# Multi-jurisdictional Privacy Compliance: Introduction

Steve Millendorf  
Donna Fraser

# Keeping Pace with Privacy

## Introduction

- Companies may be subject to privacy laws in multiple jurisdictions
- These laws can sometimes be overlapping, but still contradictory
  - Example: VA requires consent to process sensitive personal information, California doesn't require consent, but allows someone to limit the use
- Compliance with one law (such as GDPR) does NOT mean compliance with other laws (such as CPRA).
  - Despite the stated goal of CPRA that “To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions” (*Cal. Prop 24 (2020), Section 3 – Purpose and Intent*)



# Keeping Pace with Privacy

## Archetypes of Privacy Compliance Models

---

- As a result of the overlapping but potentially contradictory obligations posed by the privacy laws in different jurisdictions
- Some approaches we will discuss today:
  - Race to the top (bottom) – one set of policies and procedures based on the most stringent requirements applicable in all jurisdictions
  - Approximation – independent set of policies without adherence to any one specific policy framework
  - Selective compliance – risk based choice in terms of privacy framework and investment in compliance

PRIVACY  
LAW

CALIFORNIA  
LAWYERS  
ASSOCIATION

# Multi-jurisdictional Privacy Compliance: Race to the Top – CCPA & GDPR as the Universal Standard

Chris Ghazarian  
General Counsel  
DreamHost

# Keeping Pace with Privacy

## Which law should you follow?

---

- **Scope of business may trigger dozens of privacy laws across the world; which one applies to you?**
  - **Where are you based?**
  - **Where are your customers?**
  - **Where are your partners and consultants?**
- Tailoring laws for different segments, products, or customers is near impossible

# Keeping Pace with Privacy

## Choose the “Gold Standard”

- Pick one of the privacy frameworks with the more exacting requirements as “gold - standard” and treat all data processing activities in accordance with that standard, regardless of actual jurisdiction.

### Advantages:

- Universal accountability, Privacy by Design, Art 5 Fair Processing Principles
- Uniform management of privacy rights
- Cost (and headache) savings

# Keeping Pace with Privacy

## Be aware of non-traditional privacy rights

---

- **Certain jurisdictions may offer different (and somewhat onerous) privacy rights compared to your home base**
- **Different definitions under different acts:**
  - E.g. sensitive data under CPRA and special categories of data
- **The “Right to Rectification”**
- **Rules pertaining to protecting children**
- **Controller and Processor obligations**

# Keeping Pace with Privacy

## Unnecessary Restrictions

---

- **You may be forced to apply a legal basis where none required**
  - Create legal issues or expose company to liability?
  - Data transfers / Data processing record maintenance
  - Data Protection Officer appointment
  - Discrimination laws

PRIVACY  
LAW

CALIFORNIA  
LAWYERS  
ASSOCIATION

# Multi-jurisdictional Privacy Compliance: Approximation

Tami Dokken  
Chief Data Privacy Officer  
World Bank

# Keeping Pace with Privacy

## Pros and cons

---

- **Pros:**
  - Risk-based approach to allocating limited resources
- **Cons:**
  - Even if an organization consciously analyzes the risks vs the rewards and accepts the risks, the risks may change to unacceptable levels if (when) the business outgrows the assumed parameters - constant monitoring (and potential adjustments) is required
  - Organizations should also consider loss of good will and reputation with selective compliance approaches. May come off as “American Greed”



# Keeping Pace with Privacy

## Policy-based Compliance: Approximation

---

- The approximation approach builds a privacy program on an independent policy or set of policies that don't necessarily adhere to one specific regulatory framework.
  - E.g., World Bank Group Privacy Policy [will include link]
- Rather, this type of privacy program is a high-level framework based on common, internationally recognized data privacy and protection principles found in global regulation and global guidelines.
  - E.g., [OECD Privacy Guidelines](#)

# Keeping Pace with Privacy

## Pros and Cons

---

- **Pros:**
  - Applied on a risk-based approach that adjusts for specific, unique approaches in jurisdictions.
  - Adaptable to evolving expectations and goals.
  - Standardized, practical, single approach that reasonably meets overarching data privacy goals and objectives.
- **Cons:**
  - Risk of noncompliance with regulatory frameworks that veer away from globally accepted standards.

# Keeping Pace with Privacy

## Implementation

---

- Adopt an overarching, high-level policy.
- Implement the policy with:
  - Practical and accountable **governance** structure – who does what and when?
  - **Procedures** – how do I do what I need to do?
  - Software to **automate** and verify requirements – risk assessments, records of processing, vendor due diligence, data subject requests, etc.
- Outreach
  - Raise the **visibility** of the importance of privacy and the **value** it brings
  - Train, train, train

PRIVACY  
LAW

The logo for the California Lawyers Association, featuring a white square outline with a missing top-right corner, containing the text "CALIFORNIA LAWYERS ASSOCIATION" in white, uppercase, sans-serif font.

CALIFORNIA  
LAWYERS  
ASSOCIATION

# Multi-jurisdictional Privacy Compliance: Selective Compliance

Steve Millendorf  
Partner  
Foley & Lardner LLP

# Keeping Pace with Privacy

## Selective Compliance is NOT compliance

---

- Selective compliance is generally when a company that is in scope of one or more privacy laws only implements part of their obligations
- As lawyers, we cannot advise a client to only selectively comply with any law, including privacy laws
- That said, organizations can appropriately allocate resources to where the highest risk is or biggest bang for the buck

# Keeping Pace with Privacy

## Selective compliance does not get out of liability

- CPRA (proposed) Regulations § 7301 makes it clear that the CPPA will consider the time between the effective date of the statute/regulations, possible and alleged violations of the CPRA, and good faith efforts to comply with those regulations when deciding to pursue investigations.
  - A failure to make good faith efforts to comply with the entirety of the CPRA is likely result in increased chance of an investigation and/or civil penalties.
- GDPR Article 83 makes a similar statement – administrative fines will be based, in part, by the intentional or negligent character of the infringement.

# Keeping Pace with Privacy

## Pros and cons

---

- **Pros:**
  - Risk-based approach to allocating limited resources
- **Cons:**
  - Even if an organization consciously analyzes the risks vs the rewards and accepts the risks, the risks may change to unacceptable levels if (when) the business outgrows the assumed parameters - constant monitoring (and potential adjustments) is required
  - Organizations should also consider loss of good will and reputation with selective compliance approaches. May come off as “American Greed”

# Keeping Pace with Privacy

## Prioritization

---

- Companies subject to privacy laws in multiple jurisdictions should plan on compliance with each jurisdiction's requirement in its entirety – no “picking and choosing”
  - Some approaches have already been discussed
- While selective compliance is not likely to avoid liability, organizations can prioritize where to devote resources
- But don't shortcut by “borrowing” public facing documents of similar companies
  - Just because a competitor is in a similar business doesn't mean that their privacy practices are the same such that the privacy notice will be valid



# Keeping Pace with Privacy

## Another approach to prioritization

- GDPR lays out the structure of fines based on the EU's perceived seriousness – focus on the higher potential fines first

20M EUR/4% Violations	10M EUR/2% Violations
Basic principles for processing (consent, lawfulness, processing PI of children, special categories, criminal convictions)	Processing that doesn't require identification, children's consent, breach notification, security, ROPA's, agreements with processors
Data Subject Rights (privacy notices, access, deletion, correction, restriction on processing, objection, automated decision processing)	Obligations of certification/monitoring bodies
International transfers	
Non-compliance with an order/limitation issued by a SA	
Other obligations under member state laws	

# Keeping Pace with Privacy

## Prioritization

---

- **Priority #1:** Publicly facing documents
  - Privacy notices
  - Ability to exercise rights
  - Required Links
- **Priority #2:** Internal policies and procedures
  - Data subject request procedures
  - Formal security policies
  - DPIA
  - Contractual requirements
- **Priority #3:** technological solutions/automation

PRIVACY  
LAW

CALIFORNIA  
LAWYERS  
ASSOCIATION

# Key Components of Successful Compliance Strategies

Steve Millendorf  
Donna Fraser

Tami Dokken  
Chris Ghazarian

# Keeping Pace with Privacy

## Key Components of Successful Compliance Strategies

- **Accountability**

- Primacy of Policy – Definition of Risk- Data Life Cycle Management

- Purpose Specificity & Purpose Limitation

- *Collection of PI only for specific, explicit, legitimate and disclosed purposes*

- *No use of PI for purposes incompatible with disclosed purposes*

- (Cal. Prop 24 (2020), Section 3(B)(2) & GDPR Art. 6(4) and 13(3))*

- Privacy by Design – Smart use of DP(I)As

- Proportionality & Data Minimization

- Ensures that collection, use, and retention of PI is*

- *Reasonably necessary and*


- *proportionate*

- to achieve the purposes for which the PI was collected or processed or other compatible purposes*

- (See Cal. Civ. Code § 1798.100(c))*

# Keeping Pace with Privacy

## Key Components of Successful Compliance Strategies

- **Documentation of Privacy Practices**
    - Internal Documentation
      - Compliance Plan
        - Gap Assessment
        - Risk-based mitigation strategy
        - Resilience and Auditing
      - Record of Processing Activities // Data Mapping
    - External Documentation – Privacy Notice, Privacy Policies
      - ❖ Best Practices for Design of External Privacy Statements
        - Notice or Contract?
        - Universal or Regional?
-  CCPA: Exacting presentation requirements, not required by but not incompatible with GDPR or (See *Cal. Civ. Code §1789.130(c)* and *GDPR Art. 13*)

# Keeping Pace with Privacy

## Key Components of Successful Compliance Strategies

---

- **Organization of Privacy Operations**
  - ✓ Tiered Privacy Organization
  - ✓ Centralized privacy operations
  - ✓ Training & Audits
  - ✓ DSR/ Consumer Request Management Organization
- **Privacy Management Software –**
  - Benefits:
    - Automate risk assessments, DSRs, consent tracking, breach management, third party due diligence and contracts, etc.
    - Easier compliance monitoring
    - Ability to respond to investigations (internal, regulators, etc.)

# Keeping Pace with Privacy

## Key Components of Successful Compliance Strategies

---

- **Governance**
  - Who does what?
  - When?
  - Who decides?
  - Who is accountable?
    - ✓ E.g., RACI responsibility assignment matrix
- **Compliance Oversight and Investigations**
  - Internal or outsourced
  - Adherence to policies and procedures
  - Adherence to Codes of Conduct
  - Use of Certifications
  - Trust Agents and similar organizations

PRIVACY  
LAW

CALIFORNIA  
LAWYERS  
ASSOCIATION



Thank you



## **Tami Dokken**

### **JD, CIPP/EU, CIPP/US**

---

Tami most recently served as the first Chief Data Privacy Officer and established the first Data Privacy Office for the World Bank. She incorporated the requirements of the first Privacy Policy into the fabric of the Bank, a treaty-based organization with sovereign immunity from laws and regulations.

Previously, Tami served as Chief Data Privacy Officer and Associate General Counsel for MoneyGram International, where she developed and implemented the strategic vision for data privacy, and was chief legal counsel for sourcing, contracts, IP, and marketing. Earlier in her career, Tami was a corporate transactional lawyer for Briggs and Morgan, P.A.



# **Steve Millendorf**

## **Partner, Foley & Lardner LLP**

### **CIPP/US, CIPP/E, CIPM, FIP**

---

Steve Millendorf is a seasoned privacy and cybersecurity attorney in Foley & Lardner LLP's San Diego office. He is a partner in the firm's Technology Transactions & Outsourcing; Cybersecurity; and Privacy, Security, & Information Management Practices. With over two decades experience as an engineer, Steve's practice focusses on counseling a broad range of clients on privacy, cybersecurity, and intellectual property matters, and is recognized by the International Association of Privacy Professionals (IAPP) as a Fellow of Information Privacy and holds certifications from the IAPP as an Certified Information Privacy Professional in United States and Europe privacy laws (CIPP/US and CIPP/E), as well as an Certified Information Privacy Manager (CIPM).

Steve has a broad range of experience is assisting clients with their privacy and cybersecurity issues, including data mapping activities, data ownership and monetization, data incident management, breach response and recovery, data subject request policies and form responses, privacy notices, and the development and maintenance of various privacy and cybersecurity policies and procedure.



# Chris Ghazarian

## General Counsel, DreamHost

### Attorney, Chris Ghazarian Law

---

Chris Ghazarian is the General Counsel of DreamHost, a website, domain, and cloud company based in Los Angeles. His day-to-day includes legal, M&A, and international expansion, and he now helps shape the company's long-term strategy and goals. His experience includes managing corporations in the European Union and overseeing cross-border cybersecurity and data compliance.

Chris's legal work centers on protecting privacy in the age of big data, and with DreamHost's backing, he continues to enforce strict protocols against other tech companies, federal agencies, and international governments.

Outside of DreamHost, Chris helps his own book of clients with corporate, M&A, and IP matters, and also teaches Cybersecurity Law. He currently represents clients in a copyright infringement lawsuit against The Weeknd involving the hit song, "Call Out My Name."

