

REGULATED PERSONAL INFORMATION

---

# Privacy and Cybersecurity 101: Best Practices for Corporate Counsel to Protect Their Companies in 2024

Prepared for: Texas General Counsel Forum  
Date: December 7, 2023

## SPEAKERS

---



**KEVIN SIMPSON**

Winston & Strawn LLP  
Partner  
Litigation  
Los Angeles



**ERIC SHINABARGER**

Winston & Strawn LLP  
Associate Attorney  
Corporate  
Chicago

# Overview



# Agenda

- The Privacy Awakening: The Regulatory Landscape and How We Arrived Here
- The Driving Forces for What Comes Next
- How to Think About Managing Privacy and Security-Related Risks
- Questions

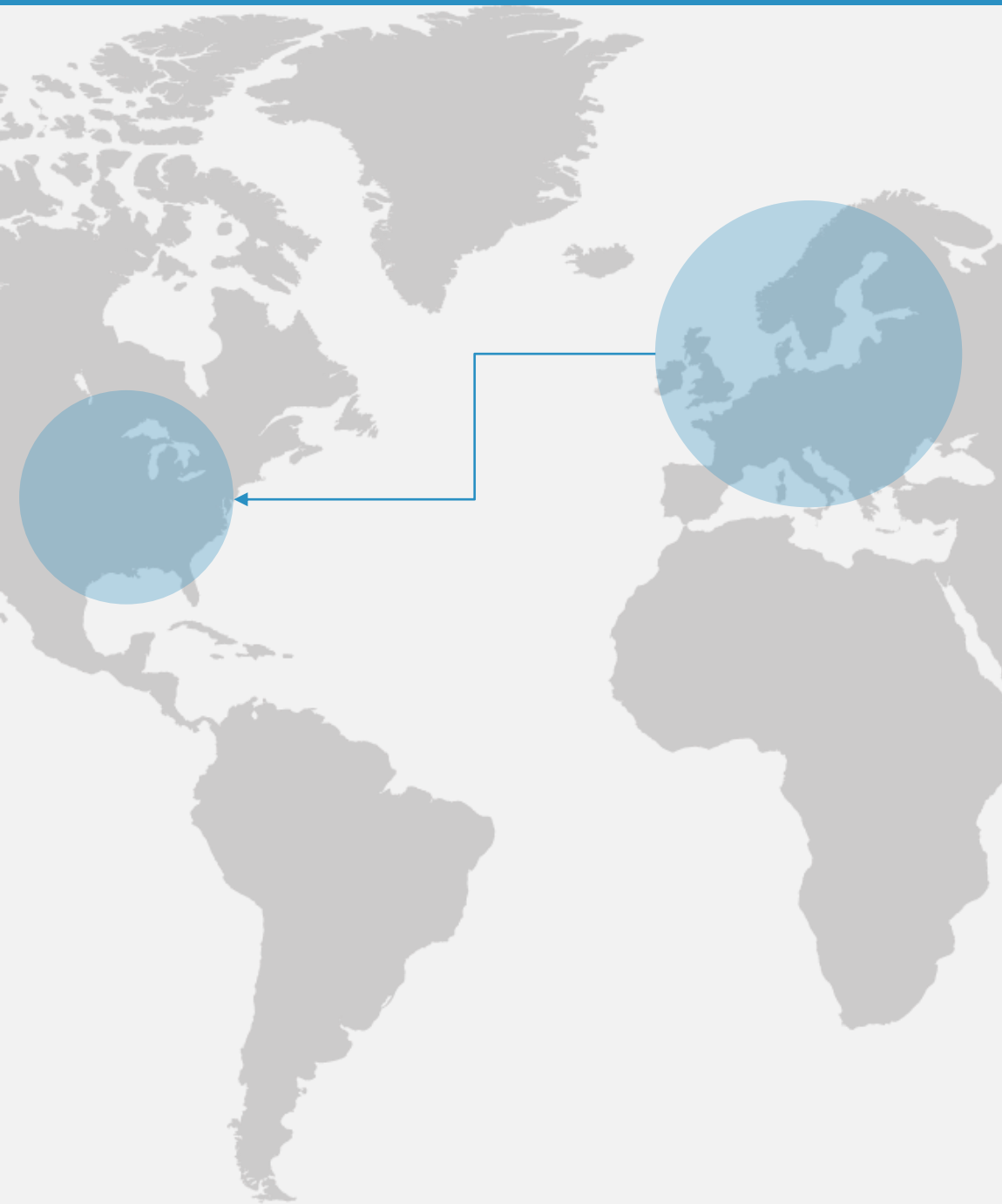


# Our Goal for Today's Presentation

- As privacy is a rapidly evolving field, there will rarely be clear-cut answers to the complicated legal questions your organization will face.
- Further, the explosion of data creation and retention creates a commensurate security risk.
- Therefore, our goal today is to provide you with meaningful context about the current state of privacy and security exposure along with a primer on how to navigate associated risks.

THE PRIVACY AWAKENING

# The Regulatory Landscape and How We Arrived Here



# How Did We Get Here?

- Europe led the way with the General Data Protection Regulation (GDPR), which went into effect in 2018 and codified long-standing European privacy principles.
- In the EU, privacy is considered a “universal human right.”
- Since 2018, regulatory fines under the GDPR have grown exponentially—including a 168% surge in fines in 2022, equating to more than US\$3.1B in fines.

# Current State of U.S. Privacy Law

- Prior to 2018, U.S. privacy regulation was focused on regulated industries.
- Regulators respond with major legislation: CCPA, CPA, CTDPA, VCDPA, etc.
- Created a patchwork of conflicting regimes that have radically shifted how businesses must manage their consumer, employee, and customer personal information.
- NY passes key regulations for financial services, data security, and biometrics.



# This Has Led to the Morass of Acronyms and Buzzwords...

Right to be “Forgotten” TCPA DNC Lists CCPA  
CIPA Prior Express Consent Written Release  
Robocalls BIPA Biometric Identifiers FSCA  
Autodialers Aggrieved Person Standard of  
Care Processing Data WESCA Personal  
Data VPPA Invasion of Privacy Aggregation  
and Anonymization

# “Americanization” of EU Privacy Regulation

- The U.S. lacks a federal generally-applicable privacy regulation akin to the GDPR.
  - The processing of personal information is governed by a patchwork of state and federal laws.
- In the last decade, U.S. legislatures have married EU privacy principles with a private right of action and statutory damages.
  - Plaintiffs’ attorneys take the bait, dusting off decades-old statutes.
- Consumers are often able to enforce U.S. privacy laws alongside regulators.

# ... And Now We Have the Perfect Storm.

- Aggressive plaintiffs' bar
- Uncapped statutory damages
- Strict liability and tough to dismiss at pleading stage
- Bet-the-business class action damages calculations
- Vague and ambiguous statutes
- Rapidly-developing case law
- Ever-changing regulatory landscape

# The Driving Forces for What Comes Next

# Trends That are Driving Change Now

Consumers want CONTROL over how their personal information is processed, and this has spurred regulators into action. In particular, consumers want to assert some authority over:

## PROCESSING

- How their personal information is collected, used, and disclosed.

## MONITORING

- What means are used to monitor their communications.

# Processing



# Increased Oversight of Processing Activities

- California, Virginia, Colorado, and Connecticut all in effect.
  - Utah joins in December 2023.
  - Texas joins in July 2024.
- CPRA regulations enforcement delayed until March 2024.
  - Regulations, including cybersecurity requirements, forthcoming.
- The CPRA and new state privacy laws increase consumer protection.
  - Create the concept of “sensitive” personal information.
  - Regulate automated decision-making.
  - Allow consumers more oversight of cross-contextual marketing.

# New State Privacy Laws

CALIFORNIA, COLORADO, CONNECTICUT, UTAH, VIRGINIA, DELAWARE, INDIANA, IOWA, MONTANA, OREGON, TENNESSEE, AND TEXAS

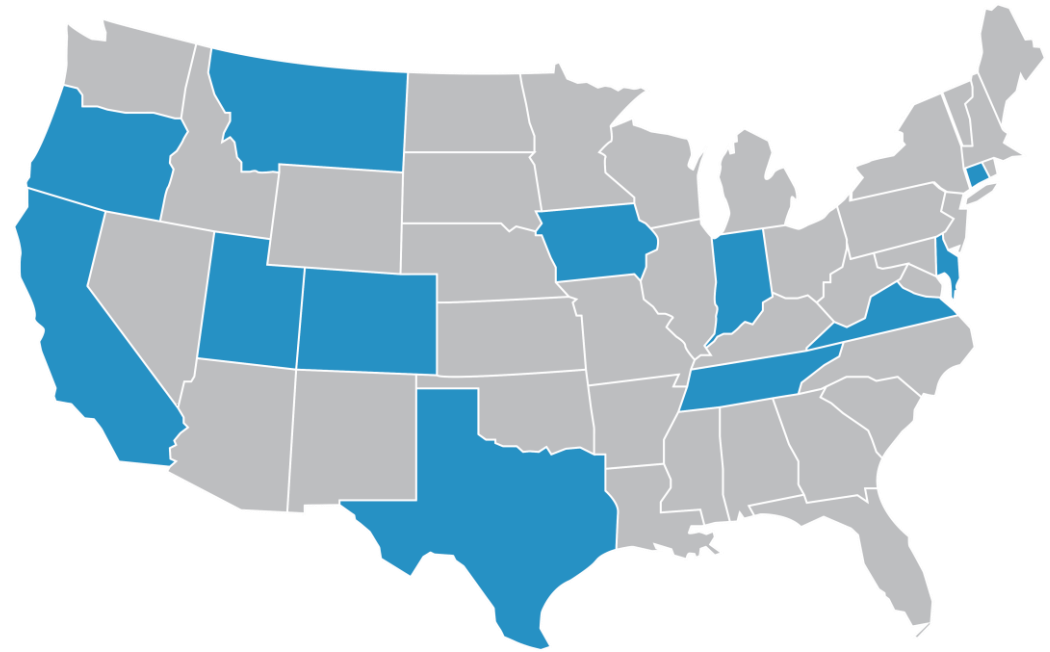
**These laws share a similar mold and are largely CPRA “light.”**  
(ex: consumer privacy rights, no private right of action)

## 2023 Effective Dates

- Virginia Consumer Data Protection Act (1/1/23)
- Colorado Privacy Act (7/1/23)
- Connecticut Data Privacy Act (7/1/23)
- Utah Consumer Privacy Act (12/31/23)

## 2024+ Effective Dates

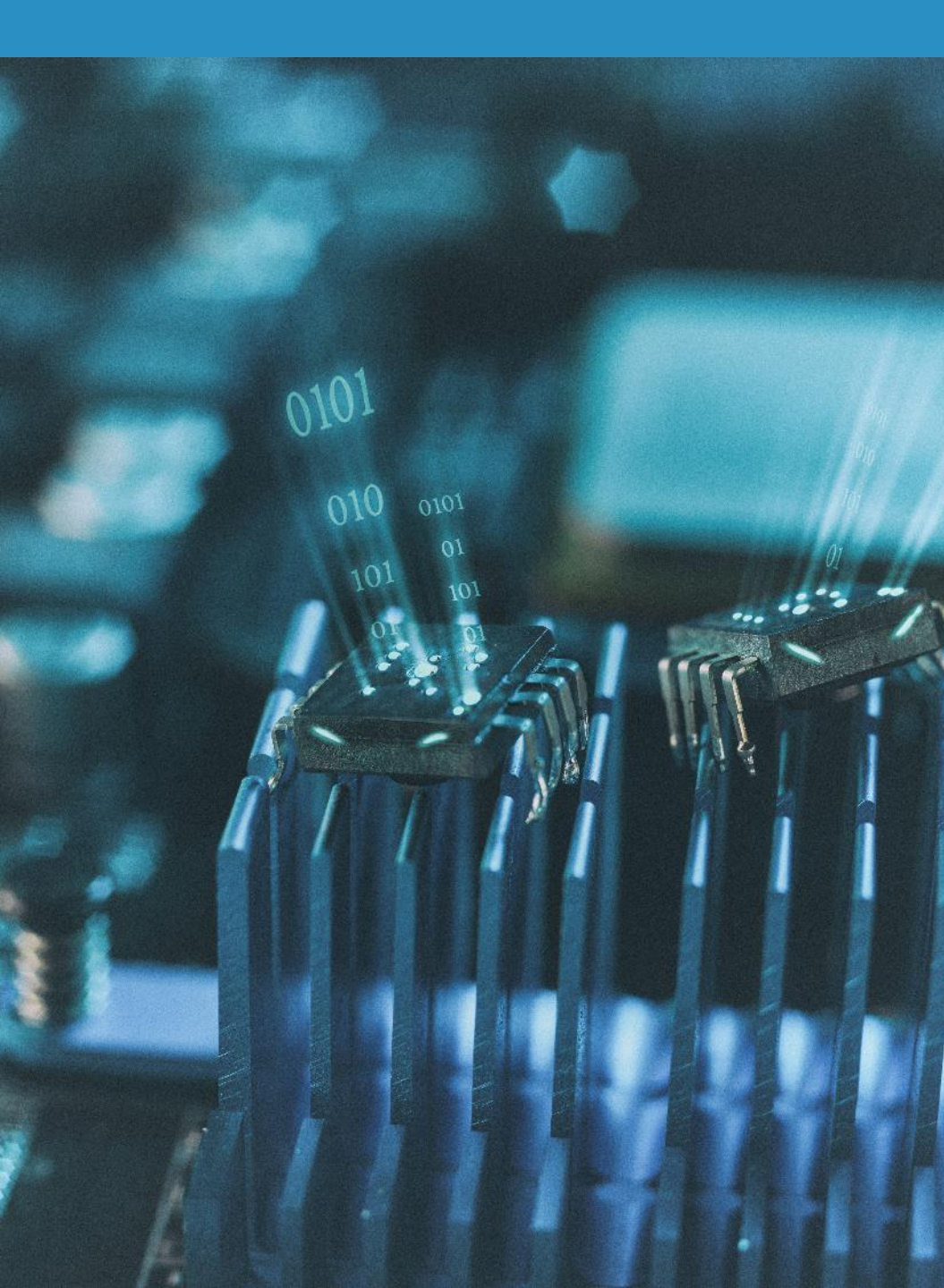
- Oregon Consumer Privacy Act (7/1/24)
- Texas Data Privacy and Security Act (7/1/24)
- Montana Consumer Data Privacy Act (10/1/24)
- Tennessee Information Protection Act (7/1/25)
- Iowa Consumer Data Protection Act (1/1/25)
- Delaware Personal Data Privacy Act (1/1/25)
- Indiana Consumer Data Protection Act (1/1/26)



# Consumer Rights Over Processing Activities

- Right to know
- Right to access
- Right to deletion
- Right to correction
- Right to opt out of the sale or sharing of personal information
- Right to limit use or disclosure of sensitive personal information
- Right to equal services and prices

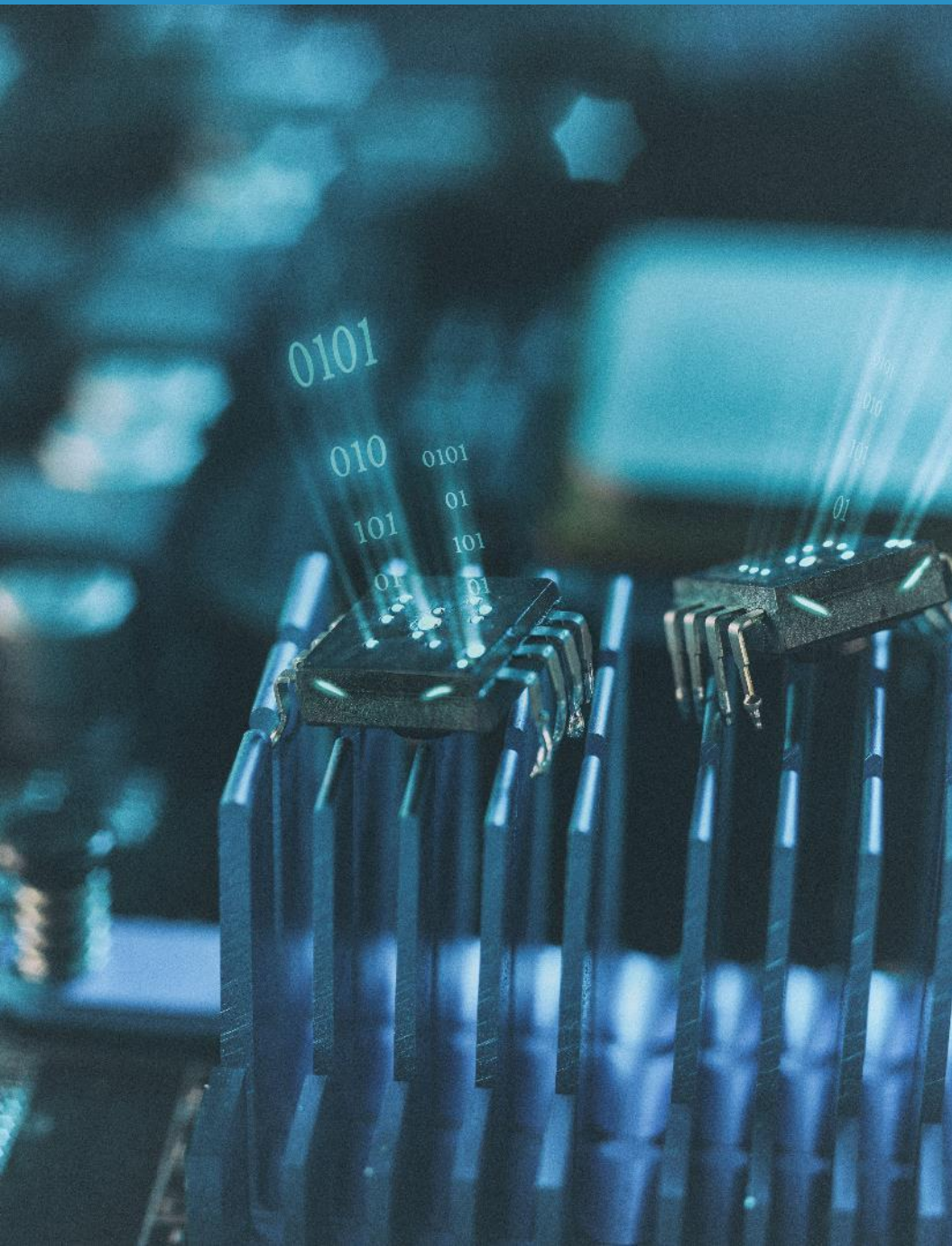
# Monitoring



# CIPA and Similar Wiretapping Laws

- Does not apply only to California organizations.
- Plaintiffs have had some success applying eavesdropping and wiretapping laws against websites using “session replay” software or passive trackers.
- CIPA prohibits intentional wiretapping or willfully learning the content of communications in transit, or attempting to use or communicate information obtained by either of those means.
  - CIPA provides a private right of action and statutory damages of up to \$5,000 per violation.
- Similar claims have been brought under other state laws.





# CIPA and Similar Wiretapping Laws

- While a website operator cannot be liable for wiretapping their own “conversations,” they may be liable for “aiding and abetting” their vendors’ “wiretapping.”
- The courts have started to show some fatigue with “tester” lawsuits against website operators.
- However, litigation remains in its nascent stage and lawsuits continue.





# Federal Video Privacy Protection Act (VPPA)

- Plaintiffs have sued website operators under the Federal Video Privacy Protection Act for use of third-party tracking tools (e.g., Meta Pixel).
- VPPA was originally intended to prevent the disclosure of personal information that identifies an individual as having requested or obtained specific video material.
  - These claims have implicated HIPAA as well, given the trackers' collection of information on websites/apps maintained by HIPAA-covered entities.
  - VPPA provides up to \$2,500 per violation.

# Texas: Laws to Watch

# Texas's Capture or Use of Biometric Identifier Act

- Requires notice and consent prior to capturing a “biometric identifier” for a “commercial purpose.”
  - Unclear whether collection of employee biometric identifiers for timekeeping purposes is “commercial.”
- Biometric identifiers must be destroyed at most a year after expiration of the purpose for collection.
- No private right of action.
  - Enforced by Texas Attorney General's office (\$25,000/violation).
  - Enforcement thus far focused on major technology companies (e.g., Facebook, Google).

# Texas Data Privacy and Security Act

- Enacted in June 2023, and goes into effect in July 2024.
- Applies to any entity that conducts business in TX, processes or sells personal data, and is not a small business.
- Similar to the CCPA in providing consumers rights, requiring vendor contract requirements, updating privacy notices, etc.
  - Will require targeted advertising opt-out technology by 2025.
- No private right of action.
  - Also has a 30-day right to cure provision.

# Enhanced SEC Cyber Requirements

# SEC Requirements for Public Companies

- The SEC finalized its cyber incident reporting rule on 7/26/23.
  - Effective in December 2023.
- Mandatory disclosure of “material” cybersecurity incidents within 4 days of determining an incident is “material.”
  - “Cybersecurity incident” defined broadly.
  - Multiple incidents may be aggregated into a “material” cybersecurity incident.
- Must also describe how they assess, identify, and manage cyber risk.



# Breach



# Breach Response

- Data breaches continue at an unprecedented rate.
- The trend continues to be for major criminal cartels “double dipping” with ransomware and data exfiltration.
- Other effects: Exposure for cybersecurity vendors and the increased costs of cyber insurance.



# Breach Litigation

- Thanks in part to CCPA's private right of action, class action litigation following data breaches has become standard.
- The CCPA's private right of action helps solve plaintiffs' standing problems.
- Statutory damages avoid the need to prove damages.

# How to Think About Managing Privacy and Security-Related Risks

# Privacy Risk is Interrelated Across the Spectrum

COUNSELING



CLASS ACTION  
LITIGATION



REMEDIATION

# Understand Where Risk Exists

- Conduct a diligence exercise to understand where your sensitive data “lives.”
- Conduct a data-mapping exercise to track how this information flows into, through, and out of your organization.
- Dispose of unnecessary data — and make sure your vendors do too.
- Talk to your business teams to assess what they are doing with personal information today, tomorrow, and two years from now.



# Address Potential Sources of Risk

- Commercial contract terms
- Oversight of vendors
- Internal understanding of privacy requirements
- Data security infrastructure
- Insurance

# Be Prepared to Act

- View data-use scenarios through the eyes of a regulator, consumer, or plaintiff's attorney.
- Undergo data security risk exercises.
- Establish processes to address privacy complaints.
- Create and execute remediation plans.

# Questions?

# Presenter Bios



#### Services

Appellate & Critical Motions  
Litigation/Trials  
Privacy & Data Security  
Privacy: Regulated Personal Information (RPI)

#### Bar Admissions

California and Illinois

#### Court Admissions

Central District of California  
District of Colorado  
Eastern District of Oklahoma  
Northern District of California  
Northern District of Illinois  
Northern District of Oklahoma  
Southern District of California  
USCA - 10th Circuit  
USCA - 5th Circuit  
USCA - Ninth Circuit  
Western District of Oklahoma

#### Education

Washington University - Saint Louis, JD  
2014  
University of Kansas, BA 2011

## KEVIN SIMPSON

Winston & Strawn Partner  
Complex Commercial Litigation  
Los Angeles  
+1 213-615-1778  
kpsimpson@winston.com

Kevin is a skilled litigator whose practice encompasses complex commercial disputes, class-action litigation, state law tort claims, and internal investigations. He has deep experience defending companies in consumer privacy lawsuits and advising companies on compliance with federal and state privacy laws.

Kevin defends and litigates complex cases at the trial and appellate levels in federal and state courts, through and including trial. While based out of Los Angeles, Kevin also has extensive involvement with the Chicago legal market.

Kevin focuses on defending class actions brought under consumer-protection and privacy statutes, including the California Consumer Privacy Act, California Invasion of Privacy Act, Telephone Consumer Protection Act, Fair Credit Reporting Act, and Fair Debt Collection Practices Act, among others. He also counsels clients to help them achieve compliance with these statutes.

Kevin has also represented federal criminal defendants by appointment. In that capacity, he negotiated plea agreements and served as first chair at trial. Kevin also regularly and energetically represents pro bono clients. He has represented an abused child in family court, mistreated inmates, and multiple asylum seekers, among others. Kevin recently obtained a jury verdict in favor of an inmate whose due process rights were denied by prison officials.

Before joining Winston, Kevin served as a law clerk for the Honorable Nancy L. Moritz of the U.S. Court of Appeals for the Tenth Circuit. Prior to clerking, he worked in private practice.

**Services**

Litigation/Trials  
Privacy & Data Security  
Privacy: Regulated Personal  
Information (RPI)

**Bar Admissions**

Illinois

**Court Admissions**

Northern District of Illinois

**Education**

Chicago-Kent College of Law, JD 2015  
Taylor University, BS 2009

## ERIC SHINABARGER

Winston & Strawn Associate Attorney  
Mergers & Acquisitions  
Chicago  
+1 (312) 558-8823  
eshinabarger@winston.com

Eric routinely advises companies on privacy and data protection issues. This includes helping companies develop comprehensive privacy and security compliance programs, monitoring and analyzing developments in state, federal, and international privacy regulation, and assisting companies in responding to potential data security incidents.

Eric is a corporate associate whose practice focuses on privacy counseling, data breach response, and regulatory compliance. As a key member of Winston's Regulated Personal Information (RPI) practice, Eric assists clients to create privacy and data security compliance programs from scratch as well as improving on existing practices. Eric's experience includes counseling clients on compliance with BIPA, GDPR, HIPAA, CCPA, CPRA, Red Flags Rule, CAN-SPAM, FCRA, GLBA, TCPA, and both state and federal unfair, deceptive, and abusive acts and practices laws. He is a member of the firm's Videogame, Gaming and Esports Group dedicated to providing comprehensive legal solutions to companies in these industries. Eric also devotes much of his practice to incident response and preparation, including preparing for and preventing data breaches, and assisting clients in evaluating and responding to threatened or actual security incidents.

Eric also regularly advises on privacy and data security matters associated with mergers, acquisitions, investments, and other significant corporate transactions. This includes handling post-closing remediation issues that implicate privacy and security and advising portfolio companies on an ongoing basis. This also includes working with clients to negotiate large-scale commercial contracts that involve the transfer, use, or security of personal information.

# Thank You

WINSTON  
& STRAWN  
LLP

