The Convergence:
Breaking Down the Old Silos of Privacy and Security

PRESENTED BY

Boltive

Spring Academy
Privacy+
Security
Forum

MODERATOR

Dan Frechtling
CEO, Boltive

PANELIST

Mason Clutter
Partner & Privacy Lead,
Frost Brown Todd

PANELIST

Chris Clymer
VP of Security
Services,
Inversion6

Introduction & Objectives

Session Overview

- Explore how privacy and security – once distinct domains – are converging due to rising data complexity, regulatory pressure, and operational overlap.

Why It Matters

- Increasing liability and enforcement
- Technology driving new forms of risk
- Privacy and security teams must now collaborate to protect data and reduce exposure

Learning Objectives

- Understand how convergence is reshaping roles and responsibilities
- Identify key drivers and real-world examples of this shift
- Review legal and operational frameworks for managing convergence
- Discuss best practices for using tools and aligning teams

# Historical Separation of Privacy & Security

Traditional Roles

- Privacy: Legal function focused on compliance and data policy

- Security: Technical function focused on protecting infrastructure

Consequences of Separation

- Misaligned goals

- Redundant or conflicting efforts

- Privacy often addressed too late in the product or compliance lifecycle

Lawyers Practicing Privacy and Cybersecurity

Privacy Lawyers (30-35K)

Cybersecurity Lawyers (10-15K)
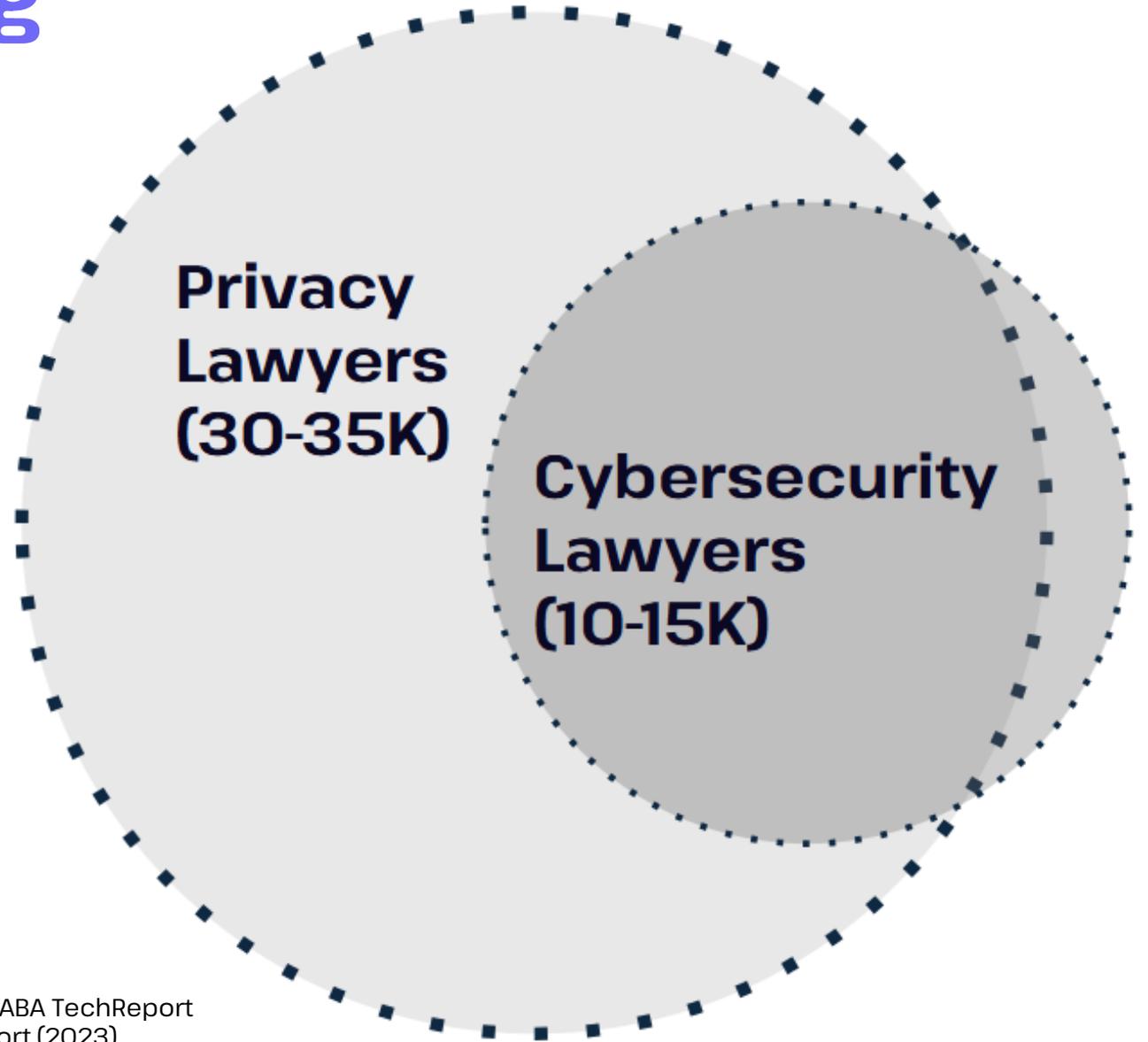
Sources: ABA Profile of the Legal Profession (2022-2023), IAPP data (2024), ABA TechReport (Privacy & Security Section) (2023), IAPP-EY Annual Privacy Governance Report (2023)

Lawyers Practicing Privacy and Cybersecurity

Cybersecurity workforce (1 million+)

Privacy and compliance workforce (50k-70k)
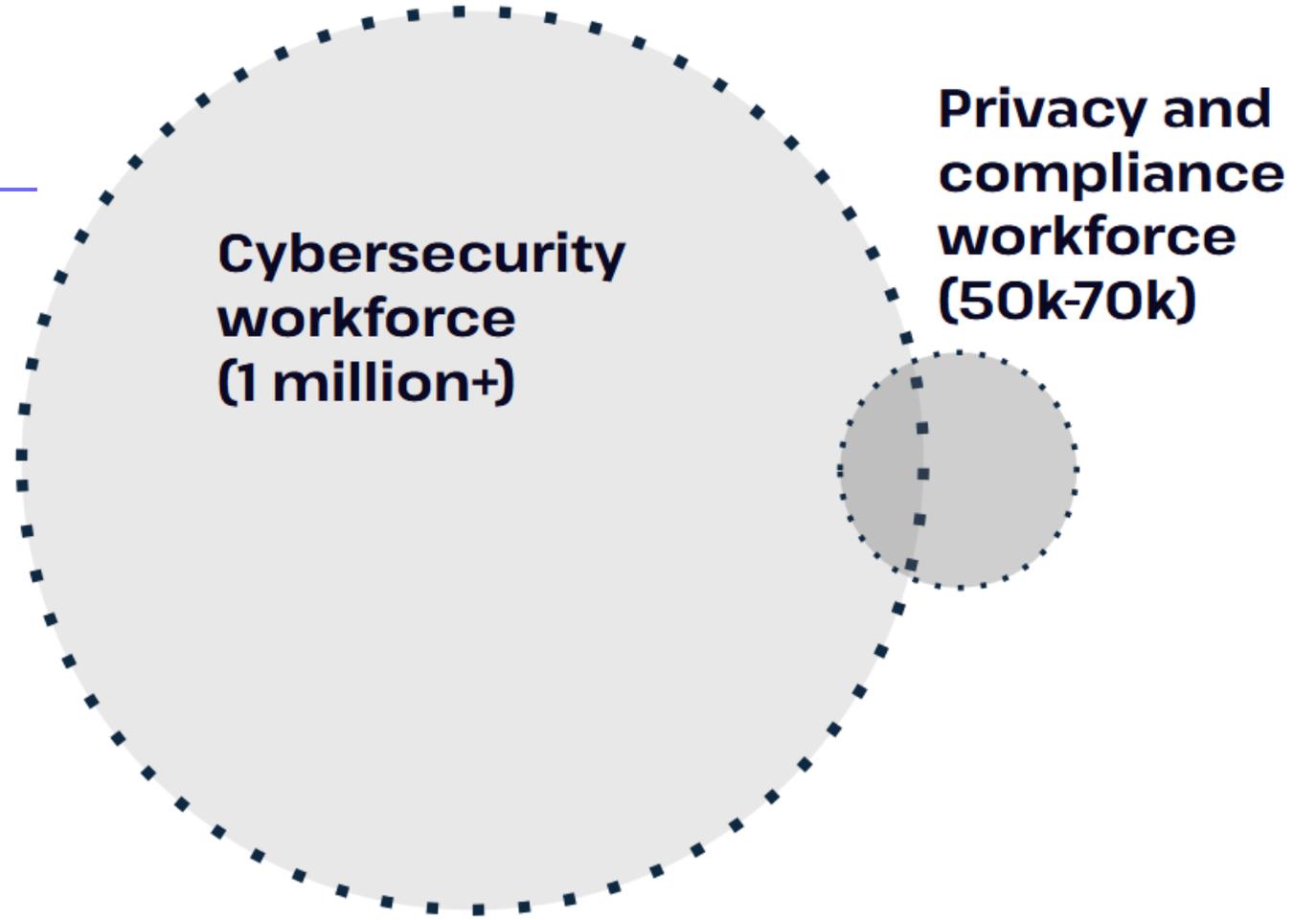
Sources: CyberSeek Cybersecurity Workforce Data (2024), Cybersecurity Ventures Jobs Report (2023), U.S. Bureau of Labor Statistics Occupational Outlook (2024), ISC2 Cybersecurity Workforce Study (2024), NIST Cybersecurity Workforce Insights (2024)

The Cost of Siloed Operations

Common Pain Points

- Security teams flag privacy issues that legal teams deprioritize

- Privacy is treated as a compliance checkbox rather than a design principle

- Late-stage involvement leads to rework, inefficiencies, and exposure

Implication

Real risk emerges when privacy and security teams don't operate from shared frameworks or priorities.
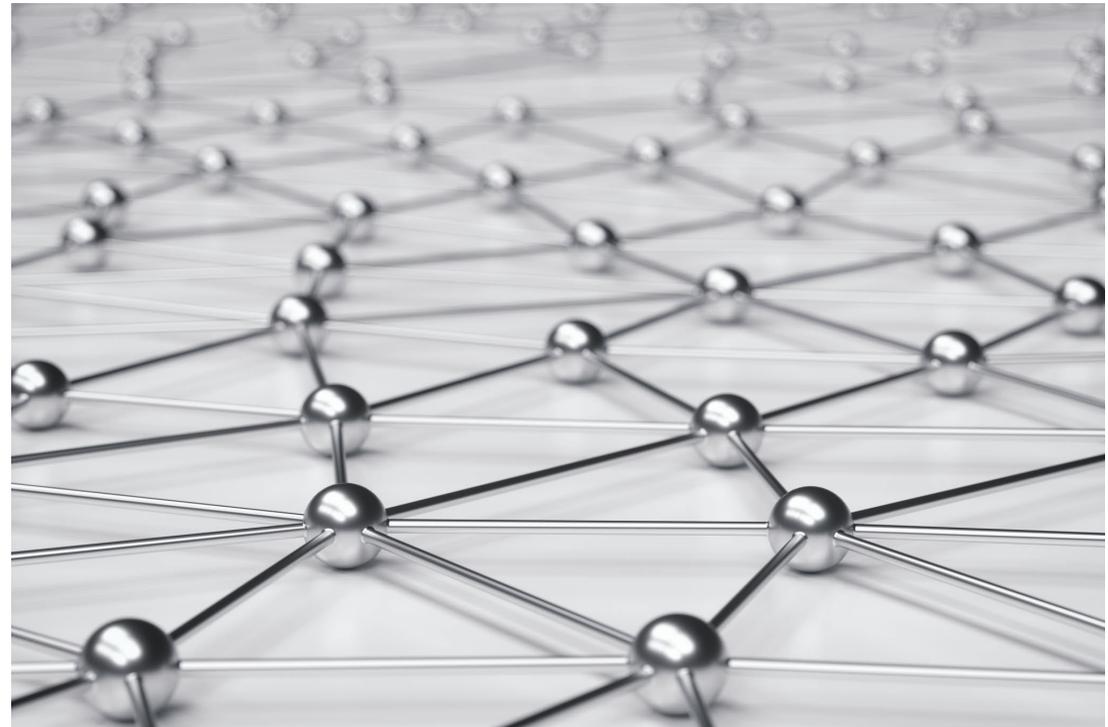
How Convergence Is Happening

Practical Examples

- Cross-functional teams are involved earlier in tech development
- Privacy and security collaborate on data governance and AI strategy
- Joint policy-making and review processes are emerging

Shift in Mindset

- From reactive to proactive
- From separate roadmaps to shared goals

Building for the Future

Key Organizational Practices

- Create ongoing dialogue between privacy, legal, and IT/security functions
- Formalize privacy-by-design as a standard process
- Coordinate budget and tool purchasing decisions
- Train teams cross-functionally on legal and technical considerations

Legal and Regulatory Frameworks

Useful Models for Practitioners and Legal Counsel

- NIST Privacy and Cybersecurity Frameworks

- ISO 27001 / ISO 27701

- FIPPs – Fair Information Practice Principles

Legal Relevance

These frameworks support legally defensible privacy and security practices and are valuable tools for advising clients or guiding internal policy.
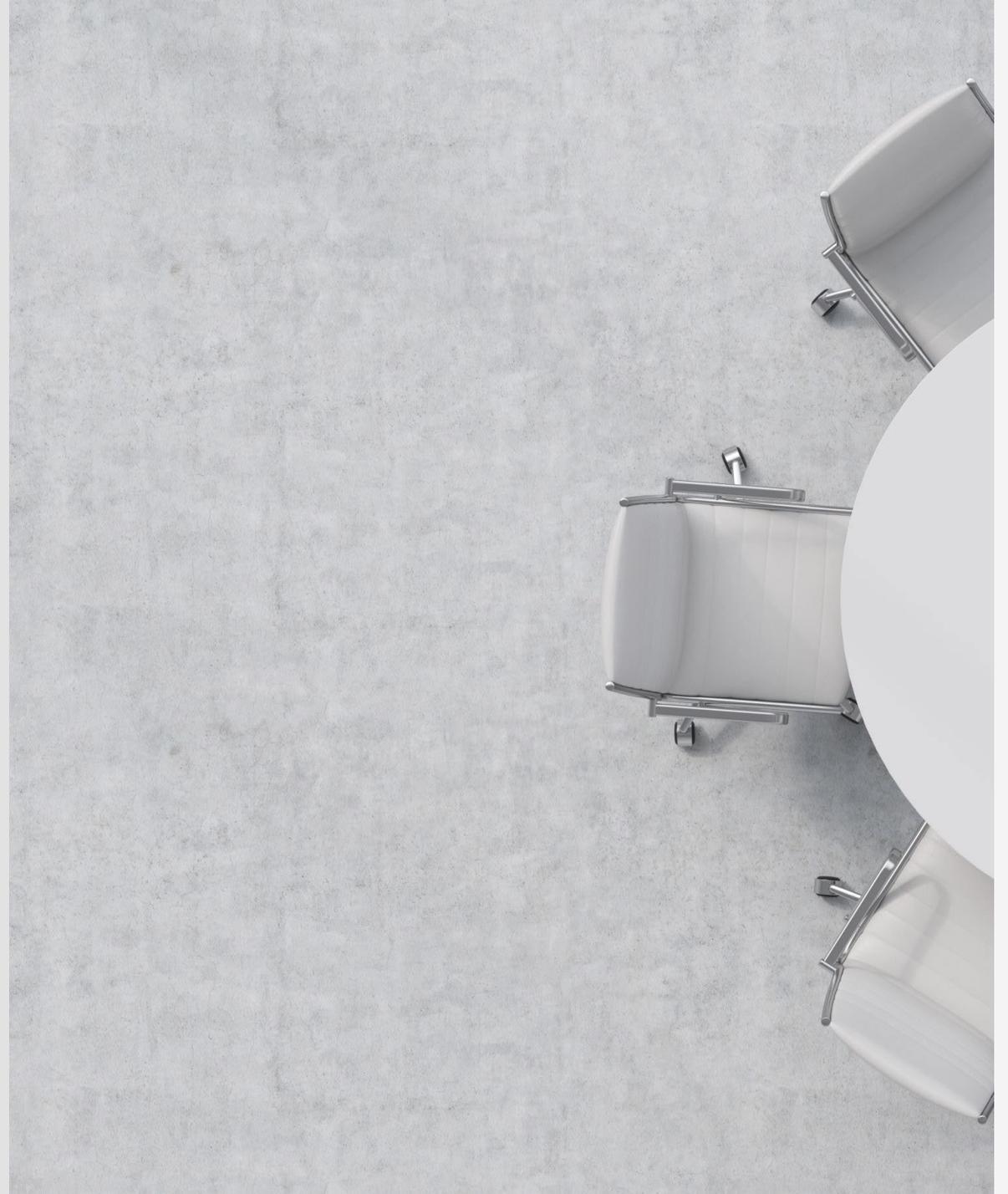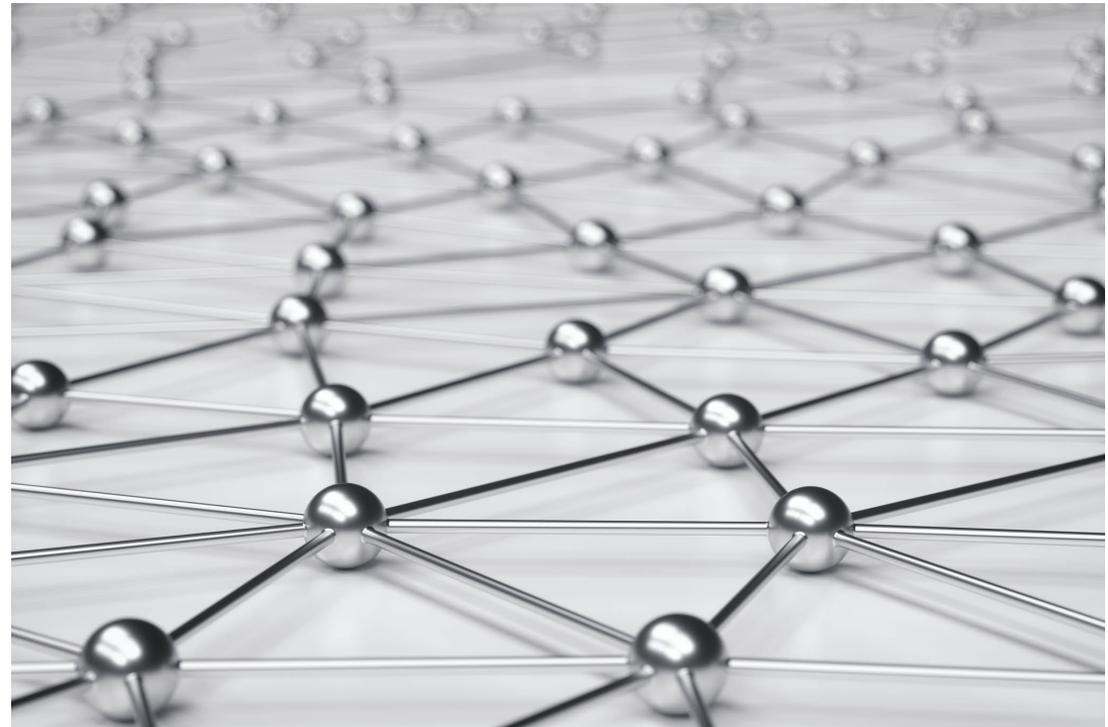
Operationalizing Convergence with Tools

Software is Not a Silver Bullet

Tools only provide value when implemented with shared goals and cross-functional alignment.

Key Advice

- Use tools to amplify aligned strategies, not to replace them
- Ensure both legal and technical teams are engaged in software adoption

Final Takeaways

Core Lessons

- Privacy and security are increasingly interdependent
- Effective convergence requires aligned goals, shared frameworks, and mutual understanding
- Organizations that build these connections early reduce risk and improve compliance outcomes

Thank you

Dan Frechtling
dan@boltive.com

Mason Clutter
mclutter@fbtlaw.com

Chris Clymer
chris.clymer@inversion6.com