FUTURE OF PRIVACY FORUM

16TH ANNUAL ADVISORY BOARD MEETING

June 11–13, 2025 • Washington, D.C.

Sovereignty, Localization, and Related Challenges to Effective Cybersecurity

Discussion Leads: John Verdi and Jocelyn Aqua

SESSION DESCRIPTION

An increasing number of regulations seek to restrict or limit organizations' ability to process data in certain countries or outside of specific jurisdictions. These restrictions are creating significant challenges in terms of managing regular data flows, contracting with data handlers, and instituting important cybersecurity measures. Join us as we discuss the current environment and help us map unanswered questions and areas of concern.

5–8 KEY DISCUSSION QUESTIONS

Regulators world-wide are erecting barriers to free data flows based on data privacy, national security/law enforcement and economic sovereignty. These rules impact how companies structure cloud infrastructure and vendor contracts, conduct cybersecurity monitoring and incident response, and design global data governance programs. Discussion will focus on recent regulatory trends, operational and contractual implications, cybersecurity and national security implications, and how companies are making strategic decisions and governing data to account for cross-border requirements.

1. **Regulatory trends:**
Which jurisdictions’ data localization or sovereignty requirements are resulting in significant cybersecurity challenges for companies today (China, India, US Data Security Program?)

Can evolving certification schemes (Global CBPR, EU Cloud) realistically improve how companies are managing data governance programs?

2. **Operational and contractual implications:**
How are organizations adapting their third-party contracts and data processing agreements to ensure compliance with localization requirements and enable effective cybersecurity? How has due diligence evolved for vendors in high risk jurisdictions? How has AI altered vendor agreements localization controls? What safeguards or provisions have been added to contracts in high-risk countries? Are SCCs, BCRs, and TIAs beneficial from a cybersecurity perspective?

3. **Cybersecurity/National Security Implications:**
How are localization and segmentation mandates affecting incident response and cyber resilience? What are the trade-offs between sovereignty and security when cross-border logging and SOC oversight are restricted? How are security teams navigating localization requirements? Are US EO/DSP and other CFIUS national security-based restrictions fragmenting cybersecurity coordination, operational silos, segmented logs, etc?

Sovereignty, Localization, and Related Challenges to Effective Cybersecurity

Discussion Leads: John Verdi and Jocelyn Aqua

CONTINUED:

1. **Strategic response and governance:**

How are organizations managing new national cybersecurity obligations, is there cross-enterprise coordination and engagement– new programs, existing cyber and privacy governance structures? How are companies prioritizing between local compliance, operational efficiency and security risk? How should CISOs, CPOs and GCs coordinate on global data strategy with business? What's the board-level view of these risks and how are they being prioritized?
What frameworks are used to evaluate data risk footprint?

How can AI governance and data localization rules be reconciled in global cloud deployments? Who owns cross-border data strategy?