Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

December 30, 2025

Entering 2026 and the Age of AI

By Amy S. Mushahwar

The New Year's Resolution: Fixing the 1999 Infrastructure Governance Problem Before Data Velocity Fixes It for You

As we enter 2026, some patterns are emerging with AI. What once failed slowly now fails at speed. Decisions propagate instantly. Harm scales before humans realize something is wrong.

2025 and the snowball effect of AI adoption is proving that artificial intelligence is no longer experimental. It is embedded in many organizations' products, workflows, analytics, and decision-making systems across industries. Boards are asking harder questions. Regulators are accelerating guidance and enforcement. Engineering teams are moving faster than governance structures were designed to handle.

Yet the central risk most organizations face is not new.

We are entering the Age of AI while still carrying unresolved infrastructure governance problems from the late 1990s (cue lyrics from the Prince song: "2000, zero-zero, party over, oops, out of time…"). Back then, systems were connected before they were understood. Data was collected before ownership was defined. Legal, security, and engineering responsibilities were fragmented. When things broke, they broke slowly.

Artificial intelligence has removed that buffer. And we are seeing a historic theme yet again.

In Y2K, the risk was rooted in a fundamental misunderstanding of how systems would behave when the numeric date flipped from 1999 to 2000. Organizations assumed continuity without fully grasping the implications of embedded logic. Today, the misunderstanding is different but equally consequential: the decentralized nature of modern data ecosystems. Data no longer resides in a single system—it flows across platforms, vendors, and automated pipelines. Artificial intelligence amplifies this complexity by consuming and generating data at scale, embedding errors and assumptions into outputs that propagate instantly. What was once a localized failure now becomes a systemic cascade.

A misconfigured access control that once meant unauthorized viewing of a few records now means an AI model trained on millions of improperly scoped data points, deployed across products, generating outputs that embed the original error at scale. Outputs influence downstream systems automatically. Errors replicate across datasets.

The problem is not that organizations lack policies. Most have them. The problem is that policies were never designed to govern modern, distributed, automated infrastructure.

As the year begins, leadership should treat this moment as an opportunity to fix what their organizations might have been deferring for decades: true data management.

Checklist of Board & Leadership Governance Imperatives for 2026

1. **Rebuild infrastructure visibility.** Confirm what data is collected, where it originates, where it flows, which systems store it, which vendors touch it, and which models consume or generate it. Infrastructure governance begins with shared visibility across legal, engineering, security, and product teams.
2. **Clarify ownership where systems intersect.** Identify who owns data at each stage of its life cycle, who owns automated outputs (who owns the output of an AI model trained on customer data, fine-tuned by engineering, deployed by product, and used to make decisions legal is liable for), and who has authority to pause or override systems when risks emerge. Accountability that fractures between teams will widen under AI.
3. **Pressure test whether infrastructure can keep the promises made in policy.** Examine whether deletion, minimization, access controls, and transparency commitments can actually be implemented across backups, logs, analytics pipelines, and training datasets. If the answer is unclear, the promise is already fragile.
4. **Align legal and engineering around the same operational reality.** Ensure legal teams understand how systems behave in practice and engineering teams understand the legal consequences of design decisions. Translation during a crisis is too late.
5. **Establish escalation paths that work under uncertainty.** Define how ambiguous signals are handled, when human review is required, who can stop automated processes, and how those decisions are documented. Governance that functions only when facts are clear will fail when they are not.
6. **Treat AI governance as infrastructure governance.** Embed oversight into architecture, access controls, logging, monitoring, and incident response rather than isolating it in policy documents or committees. Decisions must be governed where they occur, so placement of a human in the loop may be effective.
7. **Consider AI and platform safety.** Go beyond privacy and security to include safeguards against systemic risks introduced by AI and platform integrations. Evaluate model robustness, bias mitigation, adversarial resilience, and safe deployment practices. Governance should anticipate not just data misuse but also unsafe automation behaviors.
8. **Reframe board reporting toward infrastructure reality rather than compliance status.** Boards should understand where automation exists, where sensitive data flows, where failures could cascade, and where uncertainty remains. Oversight improves when leaders understand system behavior.
9. **Practice for failure before it happens.** Conduct realistic tabletop exercises that assume partial information, time pressure, and competing priorities. Include legal, engineering, product, communications, and leadership in the same room. Prepared judgment is the most valuable control in an AI environment.

The defining question for leadership in 2026 is no longer whether artificial intelligence is being used responsibly. It is whether organizations truly understand and govern the systems they have already built, now that AI has removed their margin for error.

Artificial intelligence does not reward optimism. It rewards discipline, which will not occur overnight. Discipline requires a slow-evolving, improving narrative.

The organizations that earn trust in 2026 will not be the ones with the most advanced models. They will be the ones that finally address the infrastructure governance problem they have been carrying since 1999, before data velocity forces the reckoning.

Contact

Please contact the listed attorney for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data Privacy, Security, Safety & Risk Management
T: 202.753.3825
amushahwar@lowenstein.com

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.