

US Privacy in 2026:

The Practice of Privacy Is Over

Stan Crosley

Managing Partner, Crosley Law · Red Barn Strategy

25+ years in privacy · Former Chief Privacy Officer, Eli Lilly · IAPP Westin Emeritus Fellow

MPH Data Day 2026 · April 30, 2026 · Indiana Government Center, Indianapolis

Seattle, 1962 — The Future We Imagined

- 1962 World's Fair — Century 21 Exposition
- The Space Needle, Monorail, picturephones
- IBM exhibit: mainframe computers — powerful, centralized, expert-operated, in a controlled environment

Innovation That Escapes

Atop the Space Needle

- A Five Star restaurant
- On every table is a landline phone

The Practice of Privacy is Over

- And this is where we are now.
- That work was real and was responsive to the innovations that were launched and the deferred threats we discovered. But, it was all just Practice.
- The Game is about to start.

Everything, Everywhere, All at Once

Why is today different than any other time?

**1 High Regulatory and
Enforcement Velocity**

**Dynamic Operating Model
Changes**

Unpredictable Geopolitics

**Rapidly Evolving Social &
Cultural Norms**

**Rapid Adoption of Continuously
Evolving Technology**

We'll look briefly at each of these in more detail.

High Regulatory and Enforcement Velocity

- 21+ states with comprehensive privacy; Indiana: Jan 2026. Variations are significant.
- State AI laws (CO, CA, TX, UT) – proposed in another dozen – again, key variations exist.
- No federal privacy or AI law -- state preemption seems unlikely
- Regulators are increasingly aggressive on privacy and AI enforcement.
- Civil litigation is getting extremely creative as plaintiffs use AI to generate novel complaints

Dynamic Operating Model Changes

- Demand for data within organizations is high and spiking higher – driven by a desire for data-driven decisionmaking.
- Shift to operating models with consumer/ constituent at the center – takes more data to create quality
- Healthcare (and Law?) shifting to bundled services and outcomes-based fees
- Vendor management is now essential
- Attempts to streamline workflows and org charts

Evolving Social & Cultural Privacy Norms

- Public expectations for technology have shifted dramatically over past 25 years – law significantly lags social norms, but is prompted by them.
- Children and AI: School AI deployments face the strongest public scrutiny of any government AI use case.
- Individuals now expect to use AI at work, just as they increasingly do at home – just like they expected to use their mobile phones
- Deepfake normalization
 - Changing the trust infrastructure of communication itself as synthetic media becomes harder to detect, authentication of reality becomes a privacy and institutional trust issue.
 - Government agencies that issue public communications face new obligations to authenticate and protect the integrity of those communications.

Unpredictable Geopolitics

- DOJ Bulk Data Transfer Rule
 - Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern.
- At the same time, within their own countries, government access to data is increasingly aggressive – more aggressive and less checked in EU, China, Russia, and Israel than in the U.S.
- Within the U.S. – as FTC relaxes enforcement, State AGs increase
- Executive Orders threatening to preempt state laws are met with immediate legal challenges from states and state laws that could impact constitutional rights are struck down by federal courts

Rapid Adoption of Continuously Evolving Technology

- AI is now self-recursive and algorithmically advancing
- The net effect: what you reviewed and approved six months ago, is way more capable today and as a result, creates added risk.
- Placing an infant in a play pen and using that as a safety mechanism until they are teenagers
 - Except instead of 18 years, the AI model does it in 18 weeks.

These Forces Create Risks

Data Governance Risks

- Managing risk from 21+ state privacy laws, dozens of federal privacy laws in the US, 100+ laws around the world, dozens of AI laws
- Secondary data use restrictions (often for AI dev) across jurisdictions
- Deidentification, anonymization, and pseudonymization policy harmonization
- Data mapping maturity and governance tooling (GRC platforms)
- Managing Children's, biometric, and genetic privacy requirements

Privacy and AI-Related Risks

- Ethical Data Use Principles misalignment (Safety, Fairness, Transparency, Privacy)
- Mismatch of Consumer/Individual Expectations and actual use of data by organizations
- Unachievable AI model obligations, including notice, transparency, and explainability obligations
- Data provenance failure with use for model training
- Accelerating algorithmic bias with synthetic data and model collapse
- Inadequate monitoring
- Vendor and third-party privacy and AI model risk assessment

Too Many Risks to Address

- MIT has identified 1,600 risks related to AI – that's a 200% increase in 18 months – and that's just AI.
- The key to successful data governance then, has to be, in part, quickly and adequately identifying and prioritizing risks
- This requires deep knowledge of the entity and the business area using the data/AI – Federated Governance
- If you do not have a federated data governance program, it will only get worse – the speed of this change is stunning

Governance at AI Speed: The F1 Principle

- A century of high performance engineering has taught us that governance is what allows you to go faster deeper into the corner and operate at speeds that would otherwise be reckless and life-threatening.
- The teams that will win aren't the ones who remove the brakes. They're the ones who engineer the best brakes.
- Guardrails are static and sit at a place where risk is known
- Brakes are adaptable to unknown risk and as long as braking technology advances with advancing speed, they can adequately address risk and permit organizational speed

Data Governance has to be Federated

Risk identification and prioritization requires deep contextual knowledge of the industry, entity, and business case – only SMEs familiar with the business unit and use case can be effective. No central governance process can do this.

01

PROFILE THE ENTITY

Value chain role:

Developer · Deployer · End-User

AI types in scope:

Gen AI · Predictive · Agentic

Computer Vision · Cyber AI

Industry context & regulatory
exposure (state, FTC, sector)

02

MAP AI/Data USE CASES

For each use case, identify:

- Type of AI deployed
- Entity's value chain position
- Risk tier: HIGH / MED / LOW
- Key legal & ethical risks
- Regulatory obligations triggered
- Priority governance actions

03

APPLY BESPOKE GOVERNANCE

Risk-tiered controls per use case

Accountability matrix (RACI):

Legal · Privacy · IT · BU · HR

Procurement · Internal Audit

Regulatory compliance mapping

AI impact assessments (PIAs)

Monitoring, audit & incident response

Federated Governance at AI Speed

Layering enables rapid response

ADAPTIVE FEDERATED GOVERNANCE LAYER

SME Driven · Risk Identification · Risk Prioritization · Risk Treatment · Risk Assessment

JURISDICTION SPECIFIC LAYER

Individual Data Subject Rights · Notice language · Sensitive data · Opt-outs

CENTRAL GOVERNANCE BASELINE LAYER

Data inventory · Vendor mgmt · PIAs · Breach response · Training

“The AI layer is the next floor built on the privacy foundation you already own.”

Adaptable and Scalable Data Governance: Requires Risk Tiering

Likelihood

How probable is it that this risk will materialize within the relevant time horizon?

1 = Rare | 2 = Unlikely | 3 = Possible | 4 = Likely | 5 = Almost Certain

Impact

What is the magnitude of harm to the organization, patients, or data subjects if this risk occurs?

1 = Negligible | 2 = Minor | 3 = Moderate | 4 = Major | 5 = Catastrophic

Velocity

How quickly would this risk impact the organization once it materializes?
How much response time do we have?

1 = Gradual (years) | 2 = Slow (months) | 3 = Moderate (weeks) | 4 = Fast (days) | 5 = Immediate

Risk Response: Four Strategic Options

For each prioritized risk, determine the appropriate strategic response:

Avoid

Eliminate the activity or exposure that creates the risk. May mean discontinuing a data practice, exiting a market, or declining a partnership.

Mitigate

Reduce likelihood or impact through controls, policies, training, technology, or process changes. The most common response for privacy and data risks.

Transfer

Shift the risk to another party through contractual provisions, insurance, outsourcing, or shared responsibility frameworks.

Accept

Acknowledge the risk and choose to absorb it. Must be a conscious, documented decision with clear ownership and monitoring.

Our learning is that Mitigation is attempted for far too many risks, where the risks should instead be Avoided, Transferred, or Accepted

The Real Game

In 1962, the future they imagined – orderly, observable, anticipated -- did not stay that way.

Every innovation arrives with immediate benefit. The privacy costs and other impacts came later.

Starting in 2000 and for more than 25 years, we built frameworks that sometimes felt unnecessary – like windsprints at the end of a hard practice.

But now the game is about to start and we need to rely on our practice-built skills. You are in the right room – are you ready for the game?

Background Slides

Governance Program: 11 Domains, 5 Levels

11 Governance Domains

1. Program Creation & Accountability
2. Strategic Data Governance
3. Data Breach Management
4. Training & Communication
5. Transparency, Notice & Consent
6. Collection, Use & Sharing
7. Data Subject Rights Management
8. Third-Party Risk / Vendor Mgmt
9. Physical, Admin & Technical Security
10. Data Lifecycle Management
11. Auditing, Monitoring & Enforcement

5 Maturity Levels

Level 1 — Ad Hoc

Informal, undocumented, reactive

Level 2 — Defensible

Compliance exists; not fully documented

Level 3 — Defined ← TARGET

Written, auditable, assured compliance

Level 4 — Managed/Strategic

Metrics-driven, strategically integrated

Level 5 — Optimized

Thought leader; proactive norm-setter

Most orgs: Level 1-2. 2026 demands Level 3.

Risk Mitigation Strategy & Governance Alignment

1

Review Existing Controls

Assess current mitigation efforts and control effectiveness against prioritized risks. Identify gaps between current state and desired risk posture.

2

Identify Enhanced Governance Needs

Determine where additional policies, resources, oversight structures, or technology investments are required to address top-priority risks.

3

ERM Framework Alignment

Connect privacy, data, and AI risk findings to broader enterprise risk management framework. Ensure consistent language, reporting cadence, and escalation paths.

4

Cross-Functional Federated Ownership

Assign clear risk owners across privacy, legal, IT, compliance, agency/business operations. Prioritize highest risk owners based on potential trust impact and impact to operations.

5

Segment-Specific Governance

Some units may be so significant, that they warrant separate operations to ensure they have robust controls