The Détente of Non-Compliance

Why the burden of proof cannot be met in real time, and what happens when it can

THOMAS ROCHA III
APR 20, 2026

There is a quiet equilibrium holding across the U.S. and EU right now.

It is not formal. It is not coordinated. But it is very real.

Vendors say they cannot provide real-time, in-session proof of compliance.
Regulators survey the landscape and find no one who can.
Advocates push for enforcement, but within what can be demonstrated today.

So the system settles into a working fiction:

"Document controls, demonstrate intent, audit after the fact."

That fiction is now under pressure from multiple directions at once.

The Regulatory Side Is Already There

On paper, requirements are tightening. In practice, they already have.

In the United States, the U.S. Department of Justice continues to advance ADA Title II accessibility enforcement aligned with WCAG 2.1 AA. Deadlines move, but the expectation does not: accessibility must be demonstrable in deployed systems.

At the same time, the National Institute of Standards and Technology has shifted the baseline. Session monitoring and continuous authentication are now tied directly to privacy risk and fraud detection. The requirement is no longer point-in-time validation. It is continuity.

In the EU, the pressure is more structural.

- European Commission driving implementation
- European Data Protection Board aligning interpretation
- National regulators moving into enforcement under NIS2

The European Accessibility Act has already crossed the line.
Accessibility is no longer an overlay. It is a runtime obligation.

And enforcement is increasingly indirect:

If behavior cannot be demonstrated under real conditions, it does not qualify.

The Advocacy Side Has Already Moved the Line

In parallel with regulators, pressure is coming from litigants and advocacy groups.

The NOYB, led by Max Schrems, established the pattern:

- challenge systemic behavior
- reject “best effort”
- require continuous validity

The Austrian Supreme Court ruling against Meta Platforms made that explicit.

Consent is not a one-time event.

It must remain valid continuously.

That is not a policy nuance. It is a systems constraint.

The industry still treats consent like a ticket you tear at the door.
The courts are treating it like a pulse that must be continuously valid.

Across U.S. advocacy groups, the pressure is less centralized but directionally identical:

- accessibility enforcement
- privacy and consent challenges
- AI accountability demands

Different language. Same underlying demand:

Prove what the system is doing while it is doing it.

Two Things People Get Wrong

Most of the public conversation misses two points that change the entire picture.

Schrems Is Not About Ads

The dominant framing is still:

- Facebook
- ads
- tracking

That framing is outdated.

What the NOYB cases actually established is broader:

Consent, identity, and policy must remain valid continuously during an interaction.

That applies directly to:

- SaaS platforms
- collaboration tools
- AI systems
- cloud infrastructure
- enterprise workflows

Anything that:

- maintains state
- processes user data
- evolves during execution

falls into scope.

This is why the ruling against Meta matters beyond Meta.

It is not a company-specific problem.

It is an architectural one.

Current systems cannot maintain continuous validity of consent, policy, and authority during execution.

That exposure extends across SaaS, AI, and enterprise systems, not just social platforms.

The Penalty Is Not Fines

Public discussion focuses on fines.

That is the wrong mechanism.

The real enforcement path is quieter:

systems that cannot demonstrate compliance do not qualify

This is already visible:

- U.S. procurement tied to accessibility and compliance
- EU procurement frameworks enforcing eligibility
- defense and critical infrastructure requiring a continuous Zero Trust posture

If behavior cannot be demonstrated:

- bids are not accepted
- contracts are not awarded
- systems are not deployed

This is not punishment.

It is exclusion.

Procurement gatekeeping already removes non-compliant vendors from **15 to 30 percent of enterprise ICT spend**

And that compounds:

- first government
- then regulated industries
- then enterprise environments
- eventually the broader market

The effect is not immediate.

It is cumulative.

And it is difficult to reverse.

The Vendor Reality

Vendors cannot answer the central question cleanly.

Not because they are negligent.

Because the architecture does not support it.

Modern systems are fragmented by design:

- identity in one system
- policy in another
- AI in parallel pipelines
- logs reconstructed afterward

This is the log reconstruction model.

It assumes:

behavior can be proven after the fact

That worked when constraints were independent.

They are not anymore.

Accessibility, Zero Trust, AI coordination, and data sovereignty now require:

coherence during execution

Without a unified session boundary, systems cannot:

- maintain continuous authority
- enforce policy consistently
- produce deterministic evidence

So the system falls back to:

- documentation
- partial monitoring
- reconstruction

And for now, that is tolerated.

Three Gaps Making the Problem Visible

Recent events make the structural issue observable.

The Visibility Gap

Systems cannot reliably distinguish:

- fault
- degradation

- attack

Control-plane noise and failure look the same from the outside.

Observability becomes inference.

The Trust Gap

Trust breaks outside the boundary.

The Vercel incident showed that valid tokens can represent invalid authority.

If trust ends at the token, it is incomplete.

The Intent Gap

Systems cannot demonstrate intent during execution.

Accessibility now requires real-time accommodation.

Emerging identity models separate proof from identity.

Both point to the same requirement:

Intent must be demonstrable during the interaction.

Different domains. Same failure condition.

No authoritative boundary, binding identity, policy, and execution.

Why the Equilibrium Still Holds

The current state persists because:

- no widely deployed architecture solves this
- enforcement cannot exceed capability

So the system stabilizes around:

- “no one can do this”

That is the current defense.

Why It Breaks

The equilibrium does not require a deployed solution to collapse.

It requires a credible one.

A litigant does not need to show:

- that it exists in production

Only that:

- it could exist

Once that threshold is crossed:

“impossible” becomes
“not implemented”

That is a different legal and commercial position.

The First Mover

The first credible implementation changes the landscape.

Not incrementally.

Structurally.

The first system that can:

- maintain continuous session identity
- enforce policy during execution
- produce real-time evidence

does not just improve compliance.

It establishes a new baseline.

From that point forward:

- procurement expectations shift
- liability expectations shift
- competitive positioning shifts

The reference point changes.

What Happens Next

The system is at a convergence point:

- regulatory pressure exists
- advocacy pressure is sustained
- vendor capability is insufficient

That condition resolves.

Either:

- architectures change

or

- enforcement adapts until they must

The current model cannot satisfy the requirement as written.

The Real Question

The question is no longer about compliance categories.

It is this:

Can the system prove what it is doing while it is doing it?

Right now:

No.

The moment that answer becomes yes, it shifts the balance.