

Utah Got the Identity Layer Right — Here Is What It Left Unfinished

SEDI's achievements, its deliberate gaps, and the constitutional problem that remains

Michael G. Leahy | Internet Identity Workshop | April 2026

Format: 60 minutes | ~35 min presentation / ~20 min discussion / 5 min close

Session Purpose | Establish the Utah work as the best existing state-level digital identity legislation, build credibility with the IIW community by demonstrating genuine familiarity with it, and precisely identify the three gaps it leaves open. Participants leave with a clear map of what has been solved and what has not. The gaps become the agenda for the remaining three sessions.

A. Opening and Room Calibration [5 min]

- Welcome and brief self-introduction — establish legislative background, not technical credentials
- Room identification round: name, what you work on, what brought you to this session

***Facilitator note:** Listen for the ratio of technical practitioners to policy people — it will determine how deeply you go into cryptographic specifics in Section B.*

- Frame the session: this is not an advocacy session — it is a gap analysis, and your critique of Utah is meant to be constructive
-

B. What Utah's SB260 and SB275 Actually Accomplish [12 min]

- SB260 (2025): the foundational philosophical shift
 - *Identity belongs to the individual, not the state — the SEDI concept and why this framing matters constitutionally*
 - *Anti-surveillance mandates at the point of identity presentation — no phone-home queries, no tracking of verification events*
 - *Selective disclosure as a statutory right — proving an attribute without revealing the underlying record*
 - *Explicitly a principles statute: SB260 deferred implementation, created stakeholder process, mandated study*
- SB275 (2026): from principles to operational program
 - *Digital Identity Bill of Rights — right to physical ID, right not to be compelled, right to selective disclosure, right to be free from surveillance and profiling*
 - *Optional participation with explicit anti-coercion provisions — no material benefit conditioned on digital ID adoption*
 - *Technical infrastructure requirements — key infrastructure must remain within Utah, open standards mandated*
 - *Why this is the best state-level digital identity legislation currently in existence, and why the IIW community should know it in detail*

***Facilitator note:** This section earns credibility with the room. Do not rush it. If the room skews technical, spend an extra two minutes on the cryptographic architecture implications of selective disclosure as a statutory right.*

C. The Three Gaps SEDI Explicitly Left Open [18 min]

Gap 1: The Data Relationship Beyond the Transaction

- SEDI governs the identity presentation event — the moment a citizen proves an attribute to a verifier
 - *It does not govern what government does with the vast amounts of citizen data it already holds outside that transaction*
 - *Benefits records, tax filings, licensing data, court records, health information — none of this is touched by SEDI's architecture*
 - *The government that cannot surveil the identity transaction can still maintain comprehensive dossiers through its existing systems*
- ? Does SEDI's anti-surveillance mandate extend to data government already holds, or only to the identity verification event itself?

Gap 2: The Legal Relationship — Who Is Accountable and to Whom

- SEDI establishes design principles and a bill of rights but creates no fiduciary legal relationship
 - *There is no private right of action — citizens cannot sue to enforce SEDI's guarantees without government enforcement discretion intervening*
 - *There is no framework specifying what duties government owes citizens as a matter of law with respect to data it holds outside the identity layer*
 - *Voluntary frameworks have a five-decade track record of failure — Fair Information Practice Principles have been policy since 1973*
- ? What enforcement mechanism actually backs the Digital Identity Bill of Rights when a government agency violates it?

Gap 3: The AI Decision Layer

- SEDI governs identity architecture; it does not govern what happens when AI systems make decisions from the data that architecture touches
 - *A government fully compliant with SEDI can still deploy an opaque algorithmic system to determine benefits eligibility, licensing, or enforcement priorities*
 - *The identity layer and the decision layer are distinct problems — solving one does not solve the other*
- ? If a citizen's selective-disclosure credential is presented perfectly under SEDI, but an AI system uses other government-held data to deny their benefit claim through an opaque process, what has SEDI actually protected?

D. Discussion [20 min]

- ? Has anyone in this room encountered these gaps in practice — either as implementers or as policy advisers?
- ? Is the IIW community currently working on technical approaches to any of these three gaps, and if so, where does the legal layer need to be to make that technical work viable?
- ? Utah passed both bills unanimously, in a conservative legislature, in 2025 and 2026. What does that political fact tell us about the replicability of this approach in other states?

Facilitator note: *If discussion runs long on Gap 1 or 2, let it — those are the subjects of Sessions 2 and 3. Use strong discussion here as a natural advertisement for the follow-on sessions.*

E. Close and Call to Action *[5 min]*

Bridge to Session 2: SEDI establishes what government cannot do at the identity transaction layer. What it does not establish is what government must do — and must not do — with all the data it holds outside that layer. Session 2 will present a legislative framework for that legal relationship, grounded in constitutional structure rather than policy preference.

Call to Action:

- Read Utah's SB260 and SB275 if you have not — they are short and the language is unusually precise for state legislation
- Identify one gap from today's session that your own work touches and bring a specific example to Session 2
- Share the session framework with colleagues in the digital identity space who work at the intersection of law and technology — they are the natural audience for Sessions 2 through 4