Week 3: The US privacy landscape and why it failed to protect citizens

Section 2: Privacy

Sectoral law, structural gaps, the data broker middle, and GDPR as an alternative architecture.

> **This week's central question.** The United States has dozens of privacy laws covering specific sectors, data types, and populations. If you were designing a system to fail — one that looked like protection while leaving the most consequential gaps unaddressed — would it look very different from what we have?

This week examines the structural architecture of US privacy law — not as a catalog of regulations to memorize but as a governance problem to analyze. The sectoral model produces a patchwork: organizations face different obligations depending on which state their users are in, what industry they operate in, and what category of data they hold. Organizations that comply with every applicable law can still maintain privacy postures that cause significant harm.

The Privacy Act of 1974 is examined in depth against the DOGE case. The data broker industry is introduced as the unregulated middle — the space between what the law covers and what actually happens to personal data. GDPR is presented as a structural alternative whose trade-offs illuminate what the US model has and has not prioritized.

LEARNING OBJECTIVES

By the end of this session, students will be able to:

- Identify the primary US federal privacy statutes and describe the specific gap each leaves unaddressed.
- Explain the structural difference between the US sectoral model and GDPR's omnibus approach and articulate the governance implications of each.
- Analyze a real organization's data posture and identify which laws apply, which gaps exist, and what a compliant-but-harmful outcome looks like.
- Evaluate the Privacy Act of 1974 against the DOGE case — what the law required, what happened, and what that gap reveals about enforcement architecture.
- Explain how the data broker industry operates in the space between legal regimes and why existing law has not closed that gap.
- Apply the Week 2 ethical frameworks to assess whether a legally compliant data practice is ethically defensible.

SESSION STRUCTURE

Hour 1 — The sectoral model: what it is and what it was designed to do

Open with the structural question: why does the US regulate privacy by sector rather than by right? Walk through the primary statutes using the teaching cases table — each regulation against its most consequential gap. Students should leave Hour 1 able to identify the structural logic of the sectoral model and its predictable failure modes.

Hour 2 — The Privacy Act stress test and the data broker middle

Focus on the Privacy Act of 1974 examined in depth against the DOGE case, and the data broker industry as the unregulated space all other laws collectively create. Students should articulate what the Privacy Act required, what enforcement mechanism it was given, and what the DOGE case reveals about the gap between those two things.

Hour 3 — GDPR: a different architectural choice

Present GDPR not as a superior system but as a structural alternative that forces different trade-offs into visibility. Walk through the comparison table and ask students what value each model is optimizing for. The governance implication: architectural choices in law produce architectural choices in data programs.

Hour 4 — Ethics applied to law: is legal compliance ethically sufficient?

Return to the Week 2 frameworks. The data broker case is the sharpest test: collecting, aggregating, and selling profiles on every American adult is legal. Apply consequentialist, deontological, and data justice lenses. Close by naming the course's recurring tension explicitly: governance that stops at compliance will always lag behind the harm it is designed to prevent.

Teaching cases

Regulation	Gap exploited	Case example	Governance implication
Privacy Act of 1974	No independent enforcement body; agencies	DOGE access to Treasury, SSA, IRS, OPM systems — the Privacy Act applies	A law with no enforcement mechanism is a statement of intent, not a constraint.

Regulation	Gap exploited	Case example	Governance implication
	self-report violations.	directly and is alleged to have been violated systematically.	Governance requires teeth, not just language.
HIPAA	Covers covered entities — not data brokers who purchase health data.	Data brokers legally reselling medication purchase history and mental health app data with no HIPAA obligation.	Defining coverage by entity type rather than data type creates a gap any commercial intermediary can exploit.
CCPA / CPRA	California only; no federal equivalent; employee data partially excluded.	Organizations face 15+ state privacy laws with conflicting requirements, consent mechanisms, and enforcement timelines.	Compliance with every applicable state law does not produce a coherent national privacy posture.
FERPA	Covers educational records held by institutions — not ed-tech vendors.	Ed-tech platforms collecting behavioral and biometric data on minors — the FERPA obligation attaches to the institution, not the vendor.	When processing is outsourced, coverage follows the institution. The student has no direct protection against the vendor.
GLBA	Financial institutions covered; fintech aggregators often not.	Financial data aggregators accessing bank data through APIs — GLBA obligations apply to the bank, not the aggregator.	Coverage defined at the point of original collection allows new intermediaries to operate outside the framework indefinitely.
No applicable statute	The data broker industry operates in the unregulated middle between all sectoral laws.	Acxiom and LexisNexis maintaining profiles on virtually every US adult — income estimates, health inferences, location history — with no federal law requiring consent, accuracy, or access.	The most consequential data ecosystem in the US operates with no comprehensive federal regulation. This is the result of repeated legislative inaction across five decades.

GDPR comparison — key provisions

Provision	US sectoral model	GDPR omnibus model
Legal basis for processing	No general requirement. Each sector sets different standards. Most commercial collection requires no affirmative legal basis.	Six lawful bases required (Art. 6). Every processing activity must be justified. Consent is one basis — not the default.
Individual rights	Vary by state and sector. No federal right of access, correction, or deletion for most data categories.	Universal rights: access (Art. 15), rectification (Art. 16), erasure (Art. 17), portability (Art. 20). Apply regardless of sector or data type.
Enforcement	Fragmented: FTC, state AGs, sector regulators. No single authority. Self-reporting common. Civil penalties vary widely.	Data Protection Authorities in each member state. Fines up to 4% of global annual revenue (Art. 83).
Data brokers	No comprehensive coverage. Brokers operate largely unrestricted outside California.	Covered as data controllers or processors. Subject to individual access and erasure rights.
Government data use	The Privacy Act governs federal agencies. No general restriction on government use of commercially purchased data.	Member state law governs (Art. 6(1)(e)). DPAs can investigate government processing.

Seminar discussion questions

1. The Privacy Act was passed in response to Nixon's misuse of federal data. Fifty years later DOGE suggests its protections did not hold. What does that tell us about the relationship between the political moment that produces a law and the law's durability?
2. The data broker industry is legal, largely unregulated, and maintains profiles on virtually every American adult. Apply the data justice framework: who benefits, who bears the risk, and does that distribution matter ethically?
3. GDPR gives individuals a right of access, rectification, and erasure. The US does not recognize those rights federally for most data categories. Is that a privacy failure, a policy choice, or both — and how do you distinguish between them analytically?

4. An organization complies with every applicable US privacy law but its practices cause measurable harm to a specific population. Construct the strongest ethical argument that it has done nothing wrong — then construct the strongest argument that it has.
5. The US has attempted comprehensive federal privacy legislation multiple times without success. What would need to change for a federal law to pass — and would it close the gaps this week identified?

Course thread

Coming from — Week 2 gave students ethical frameworks to evaluate data decisions beyond legal compliance. They arrive in Week 3 ready to apply those tools to the law itself.

Going to — Week 4 moves from law to engineering, asking how privacy protection gets built into systems rather than bolted on after the fact.

Required

Required reading

- Daniel Solove and Paul Schwartz, Privacy Law Fundamentals (current edition) — chapters covering the Privacy Act, HIPAA, GLBA, and FERPA. Approximately 50 pages.
- Danielle Citron, "DOGE Betrays Foundational Commitments of the Privacy Act of 1974," Lawfare (February 2025) — approximately 8 pages. Primary analytical text for Hour 2.
- Lothar Determann, Determann's Field Guide to Data Privacy Law (current edition) — GDPR chapter only, approximately 25 pages.
- Pam Dixon and Robert Gellman, "The Scoring of America" (World Privacy Forum, 2014) — executive summary and data broker section, approximately 20 pages.

Recommended reading

- Chris Jay Hoofnagle, Federal Trade Commission Privacy Law and Policy (2016) — chapter 1. The FTC's role as de facto privacy enforcer in the absence of a general privacy law.
- Paul Schwartz and Karl-Nikolaus Peifer, "Transatlantic Data Privacy Law" (2017) — deeper comparative analysis of US vs. EU approaches.
- Privacy Rights Clearinghouse, "Data Brokers: A Call for Transparency and Accountability" — accessible overview of the data broker ecosystem.

Assignment

> Enter the course code to unlock assignments.