PRIVACY & AI LAW — S06E04

NAVIGATING THE US PRIVACY PATCHWORK (CCPA/CPRA, GPC & STATE LAWS)

FOR: FOUNDERS, PMS, DEVELOPERS, AND MARKETERS

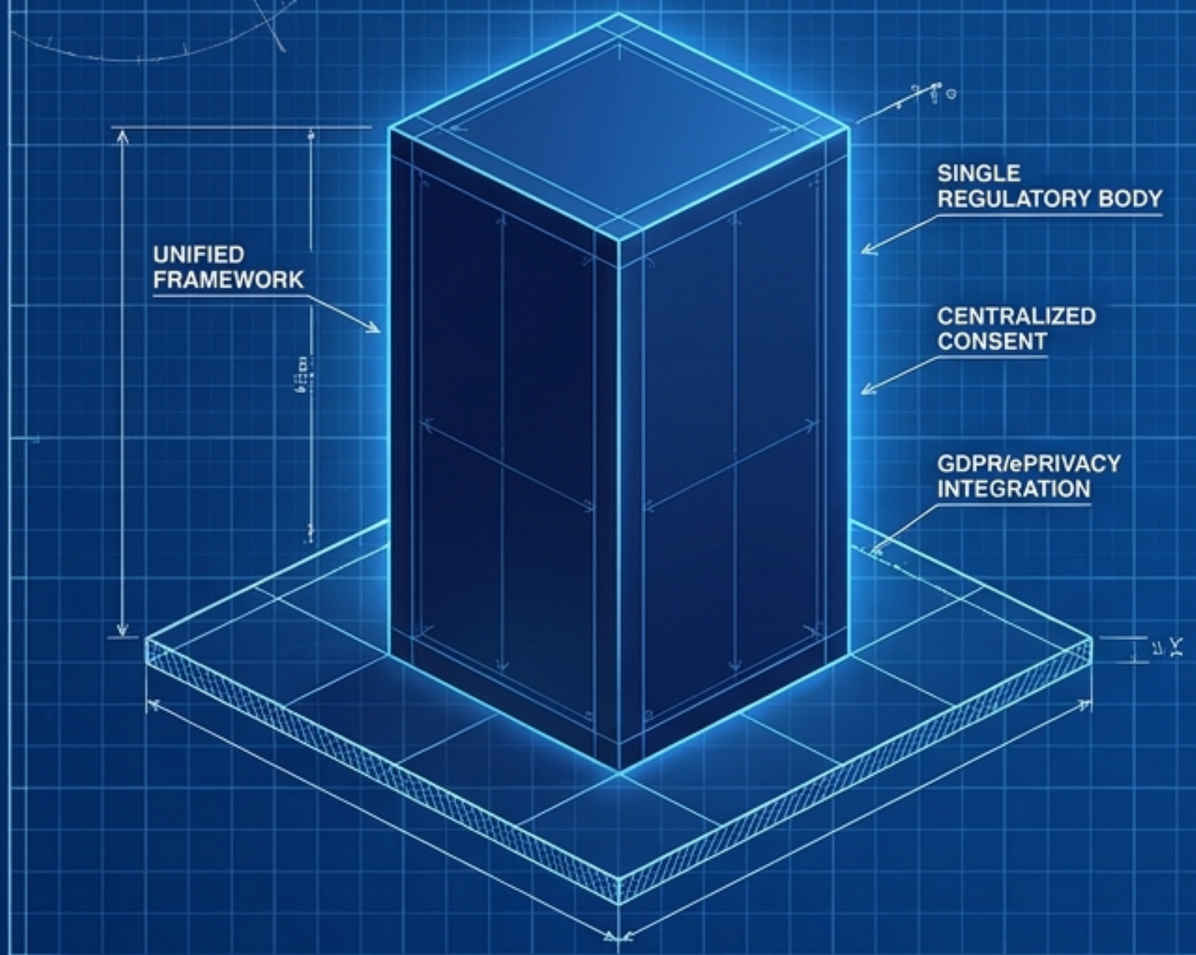


MANDATORY DISCLAIMER: GENERAL INFORMATION, NOT LEGAL ADVICE — CURRENT AS OF NOVEMBER 2026.

Gemini Notebook

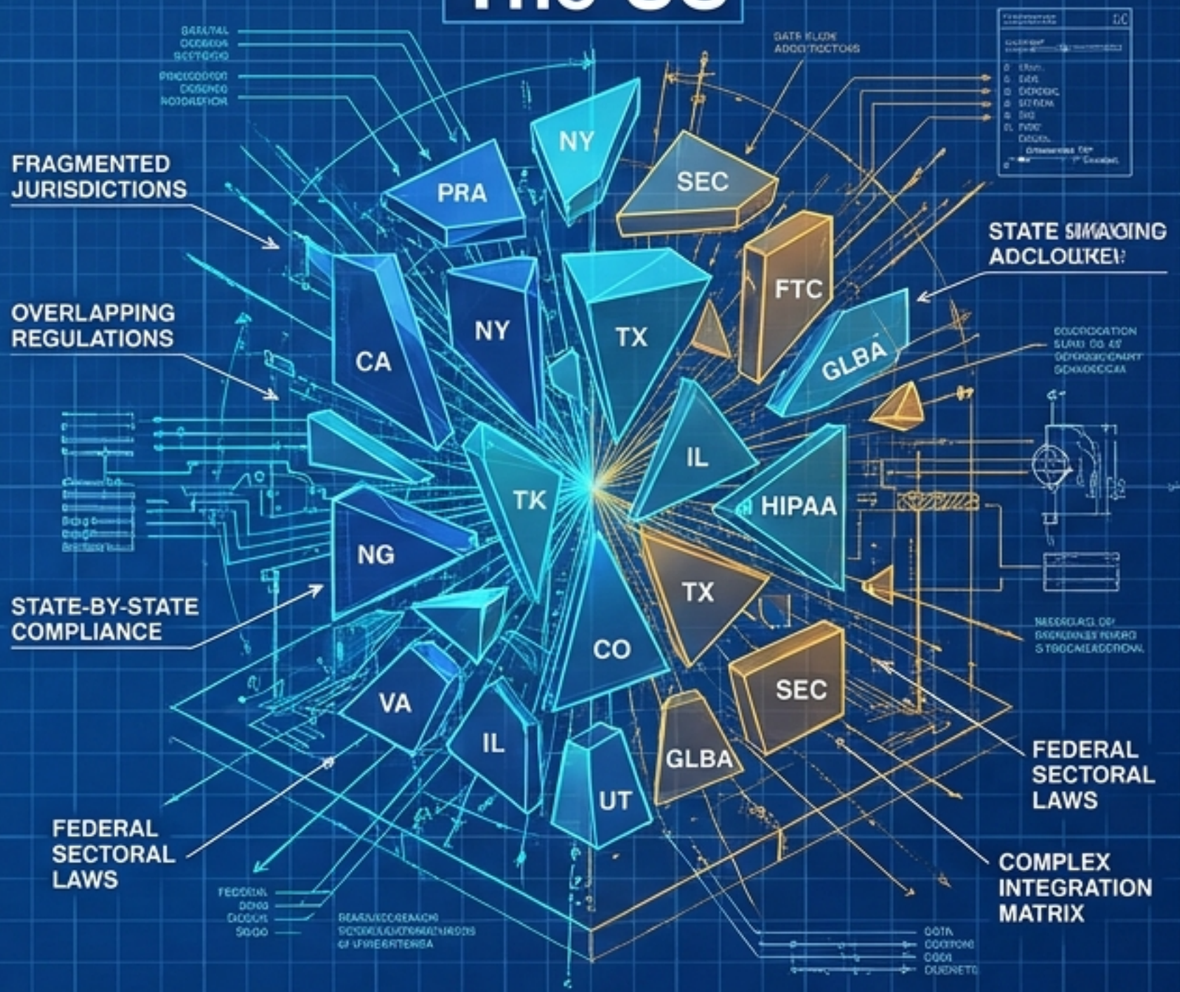
The Free-for-All Myth

The EU



Episode 3 Recap: The EU relies on centralized ePrivacy opt-in banners and a singular, unified GDPR regime.

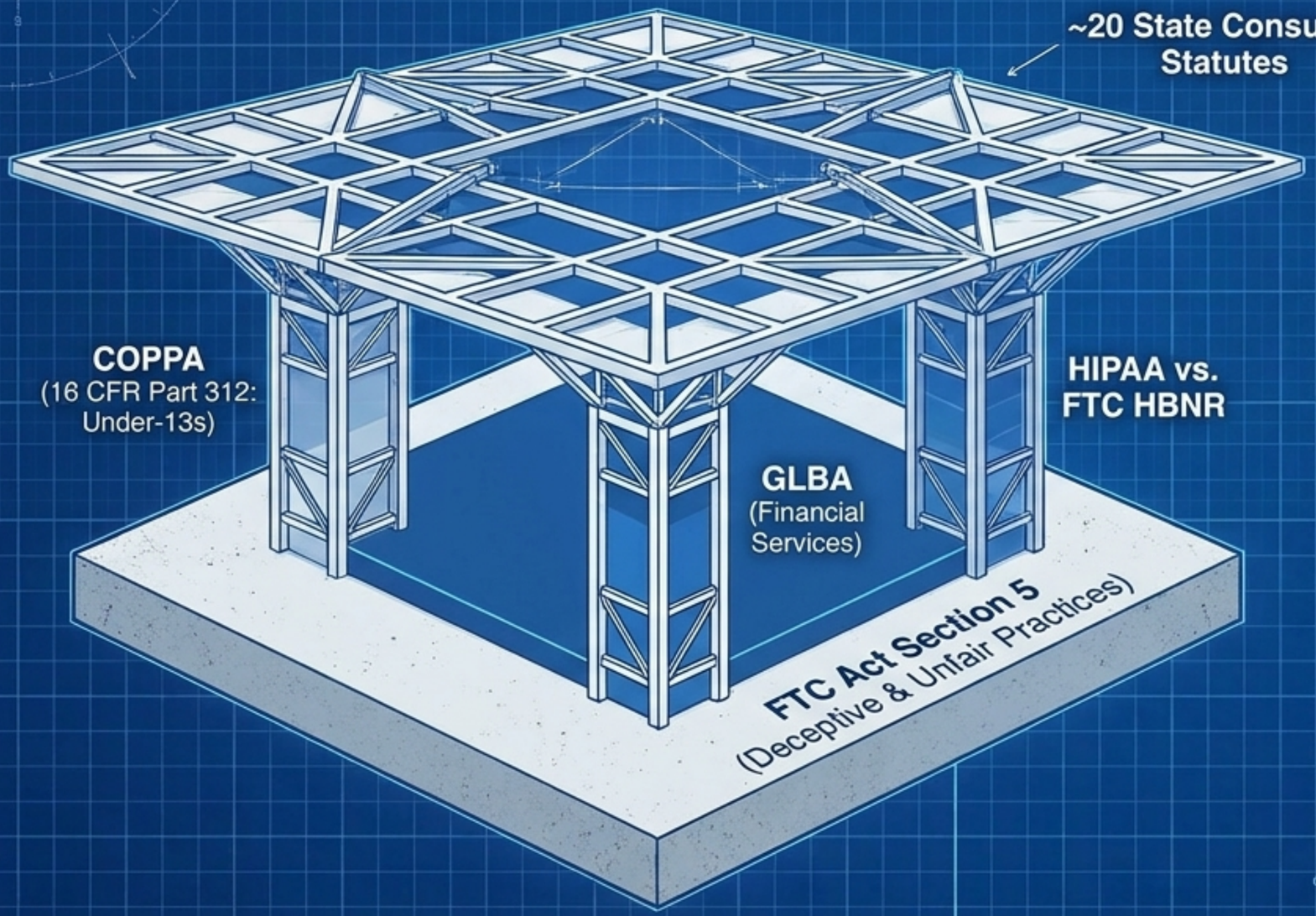
The US



The Reality: The absence of a federal law does not mean a free-for-all. Product teams must engineer for a heavily fragmented patchwork of overlapping federal and state jurisdictions.

Gemini Notebook

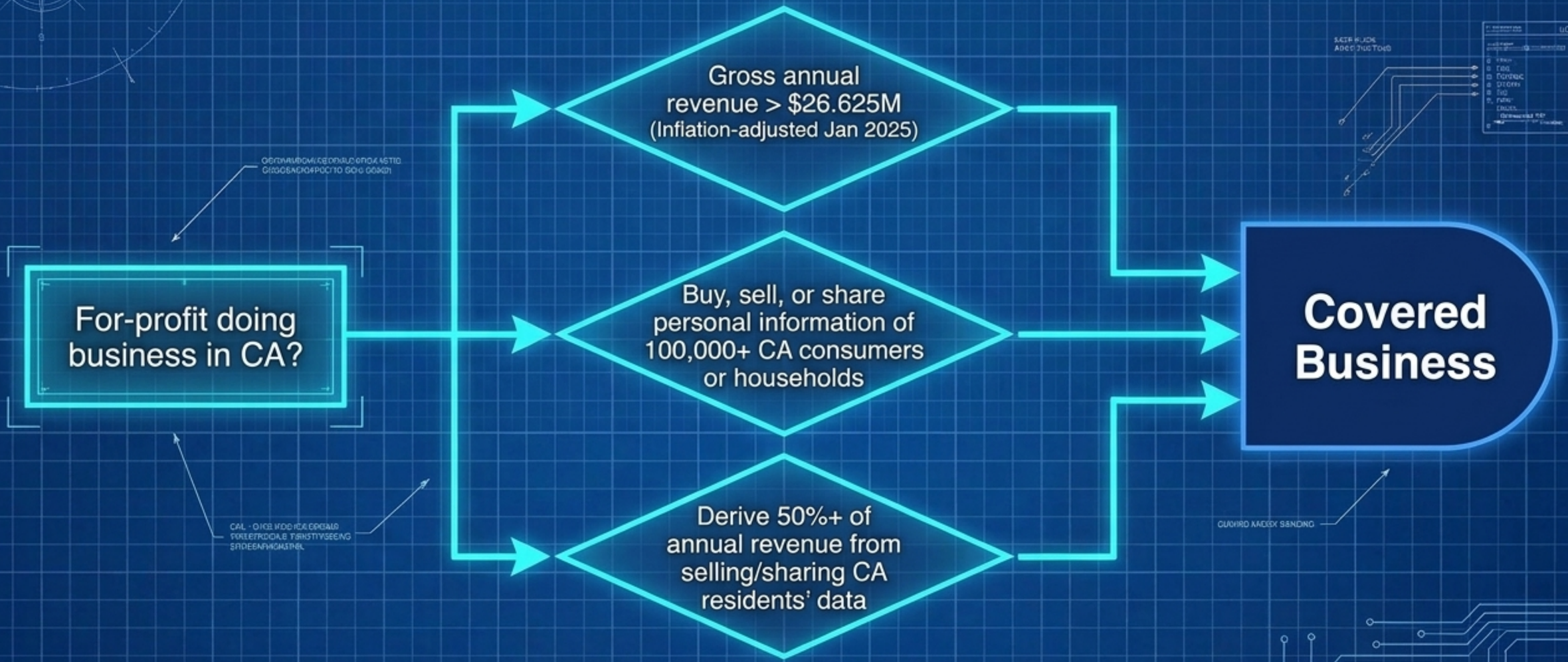
The US Privacy Architecture



Key Takeaway: US privacy isn't one law. It is a foundational federal enforcement mechanism supporting specific industry pillars, overlaid with a dense canopy of state-by-state consumer rights.

Gemini Notebook

CCPA/CPRA: Are You a Covered Business?

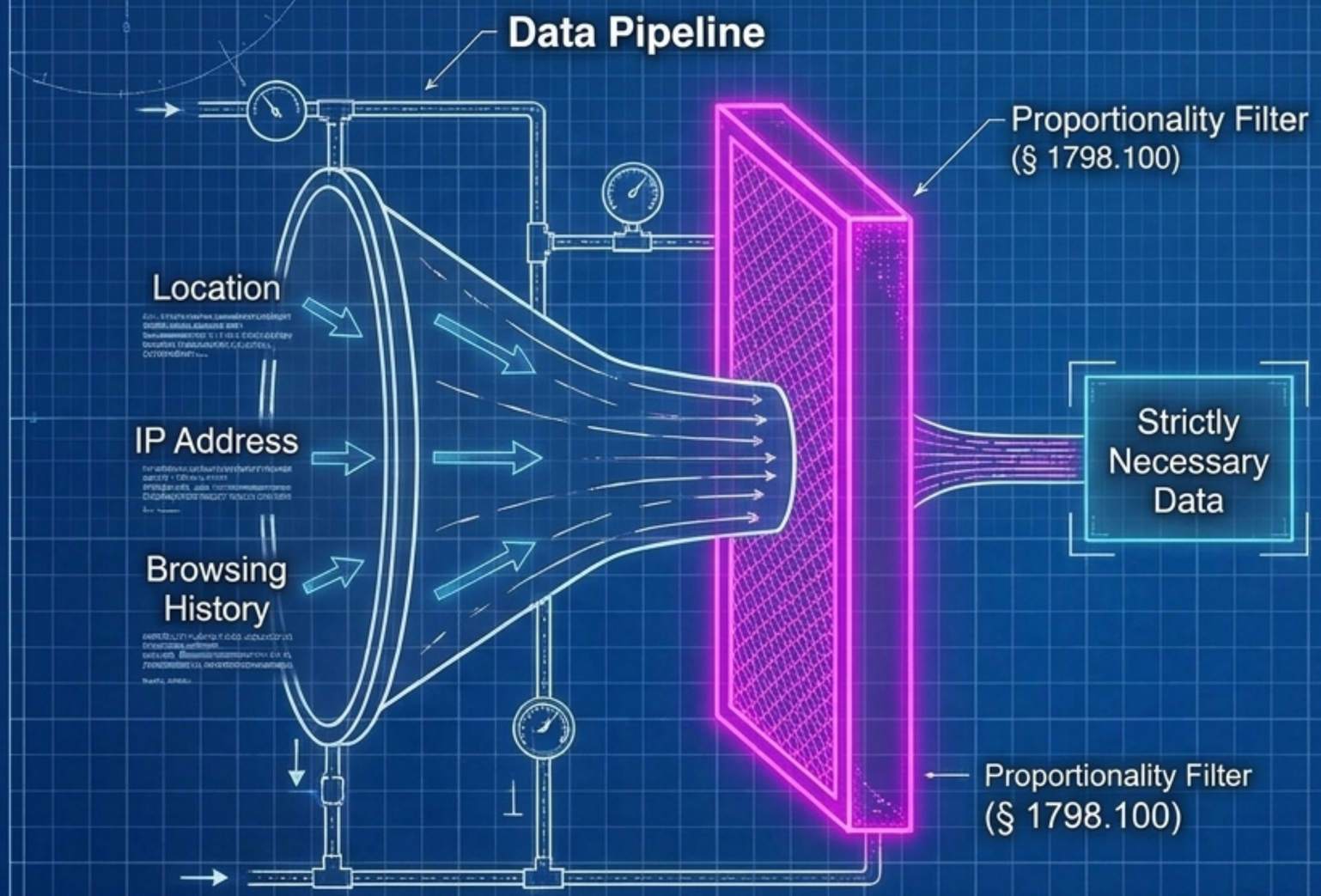


⚠ WARNING

Threshold Logic: Cal. Civ. Code § 1798.140(d). Hitting JUST ONE of these thresholds triggers full compliance obligations.

Gemini Notebook

The Notice & Minimization Mandate



The Legal Code

Cal. Civ. Code § 1798.100 & CPPA Advisory 2024-01 requires data collection to be reasonably necessary and proportionate.

The UX & Architecture Translation

Notice at Collection must occur at or before capture. The system must natively reject excessive data collection that does not align with disclosed, compatible product functions.

Gemini Notebook

The Full Suite of CCPA Consumer Rights



Right to Know

Disclose categories and specific pieces of PI.



Right to Delete

Wipe data. Integrates with upcoming SB 362 Delete Act DROP single data-broker platform (Jan 2026).



Right to Correct

Amend inaccurate personal information upon request.



Right to Opt-Out of Sale/Sharing

Stop data transfers. Strict affirmative opt-in rules apply for users under 16. (§ 1798.120)



Right to Limit Sensitive PI

Restrict secondary uses of precise geolocation, biometrics, etc. (§ 1798.121)

⚠ WARNING

CCPA/CPRA compliance requires integrated systems for all rights. Failure to comply can lead to significant penalties. § 1798.150, § 1798.155

Gemini Notebook

Expanding Enforcement: The CPPA Radar



Regulatory Reality: The CPPA (California Privacy Protection Agency) acts as a dedicated privacy police force with audit and enforcement powers. It is not waiting for consumer lawsuits to act.

Gemini Notebook

State vs. EU Diagnostic Matrix: Thresholds & Applicability

Jurisdiction	Covered Entities	Revenue Threshold	Data Vol. Threshold	Exemptions
EU (GDPR)	All processing data	None	None	Household use
CA (CCPA)	For-profits	> $26.625M	100k consumers/ households	GLBA, HIPAA
VA (VCDPA)	For-profits	None	100k consumers	GLBA, HIPAA, Non-profits
CO (CPA)	For-profits	None	100k consumers	GLBA, HIPAA, Non-profits
CT (CTDPA)	For-profits	None	35k consumers	GLBA, HIPAA, Non-profits
OR (OCPA)	For-profits & Non-profits	None	100k consumers	HIPAA
TX (TDPSA)	All conducting business	None (SMEs exempt)	None	GLBA, HIPAA

Unique to OR

Revenue caps dropped

⚠ WARNING

Gemini Notebook

State vs. EU Diagnostic Matrix: Engineering Defaults

Jurisdiction	Default Processing Model	Universal Opt-Out / GPC	Enforcement / Cure Period (IAPP)
EU (GDPR)	Strict Opt-In	N/A	Immediate
CA (CCPA)	Notice-and-Opt-Out	Mandatory	Discretionary
VA (VCDPA)	Notice-and-Opt-Out	Not Required	30 Days (Discretionary)
CO (CPA)	Notice-and-Opt-Out	Mandatory	60 Days (Sunsets 2025)
CT (CTDPA)	Notice-and-Opt-Out	Mandatory	60 Days (Sunsets 2025)
OR (OCPA)	Notice-and-Opt-Out	Mandatory (Jan 2026)	30 Days (Sunsets 2026)
TX (TDPSA)	Notice-and-Opt-Out	Mandatory (Jan 2025)	30 Days

Core Takeaway: The US is largely a Notice-and-Opt-Out regime, diverging sharply from the EU. However, mandatory engineering support for automated GPC signals is rapidly becoming the national baseline.

⚠ WARNING

Gemini Notebook

The Sensitive Data Divide

California: Right to Limit (§ 1798.121)



Consumers can opt-out after the fact.

VA/CO/CT/TX: Affirmative Opt-In



Strict barrier. Data cannot be collected without prior consent.

Sensitive Data Definition: Includes precise geolocation, health/biometrics, race, genetics, and under-13 data. (**Note:** CTDPA explicitly includes Consumer Health Data and neural data).

Product Architecture Rule: Building a unified US app requires defaulting to the strictest standard—build an upfront opt-in flow for sensitive data to satisfy VA/CO/CT/TX, which automatically complies with CA.

⚠ WARNING

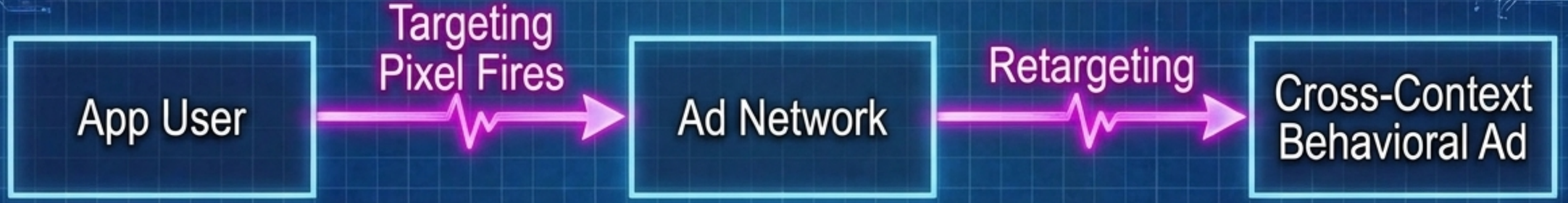
Gemini Notebook

Sell vs. Share: The Engineering Translation

Traditional "Sale"



CCPA "Share" (§ 1798.140)



Key Insight: You do not have to exchange money to sell or share data under California law. Firing a standard marketing pixel to retarget users across other websites constittutes sharing for cross-context behavioral advertising, instantly triggering strict opt-out requirements.

⚠ WARNING

Gemini Notebook

The Vendor Contract Trap

Legal Status:
THIRD PARTY
(Triggers Opt-Out Rights)

```
"vendor_config": {
  "vendor_name": "AnalyticsSDK",
  "data_access": "Full"
}
```

```
"vendor_config": {
  "vendor_name": "AnalyticsSDK",
  "data_access": "Strictly limited to requested services",
  "mandatory_statutory_clauses": true
}
```

Legal Status:
SERVICE PROVIDER / CONTRACTOR
(Safe)

Actionable Rule: Engineers cannot integrate new SDKs or APIs without Legal confirming the vendor is contractually bound as a Service Provider. Otherwise, the data transfer is a ‘Sale’ or ‘Share’.

⚠ WARNING

Gemini Notebook

GPC Under the Hood: Frictionless Compliance

Backend (Network Level)

```
HTTP Request Headers
Host: api.product.com
User-Agent: Mozilla/5.0...
Sec-GPC: 1
```

Frontend (DOM Level)

```
> navigator.globalPrivacyControl
  true
```

Legal Mandate (CCPA § 1798.135 & CO/CT): Businesses must automatically honor the Global Privacy Control (GPC) signal as a valid opt-out of sale/sharing without requiring additional user friction.

Design Rule: Do not show a pop-up asking the user to confirm their GPC signal. Read it at the network or DOM level and automatically suppress tracking pixels.

⚠ WARNING

Gemini Notebook

Autopsy of an App: A Worked US Scenario



Scenario Setup: Pulse App

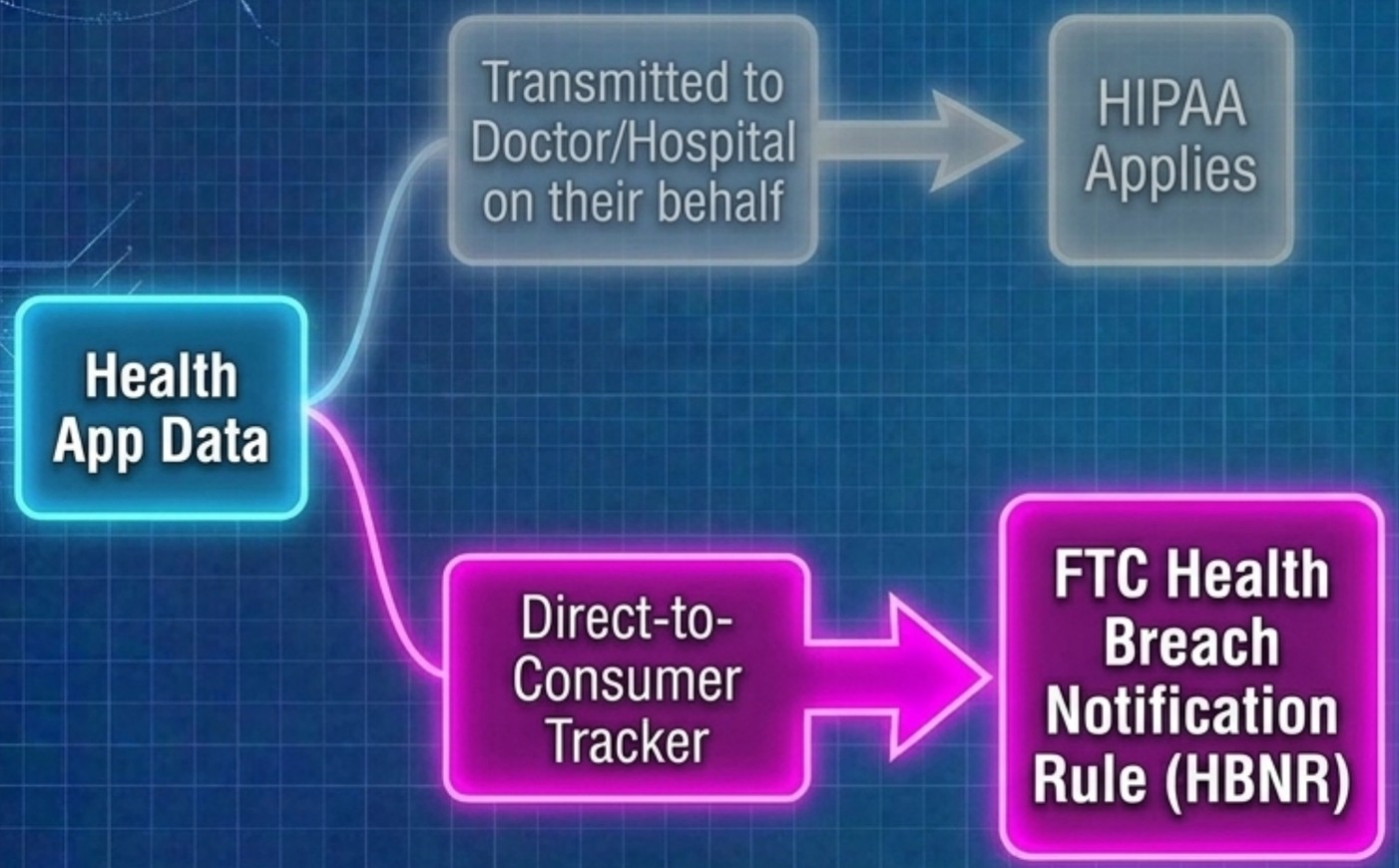
- **Product Category:** Consumer health, diet, and lifestyle tracker.
- **Scale:** Just crossed 100k users in California; preparing for a massive nationwide marketing push.
- **Monetization:** Premium subscriptions + ad-supported tier.

The Goal: Map the data flows to identify exactly where the app steps on regulatory tripwires across the US patchwork.

⚠ WARNING

Gemini Notebook

The HIPAA Illusion vs. The FTC Reality



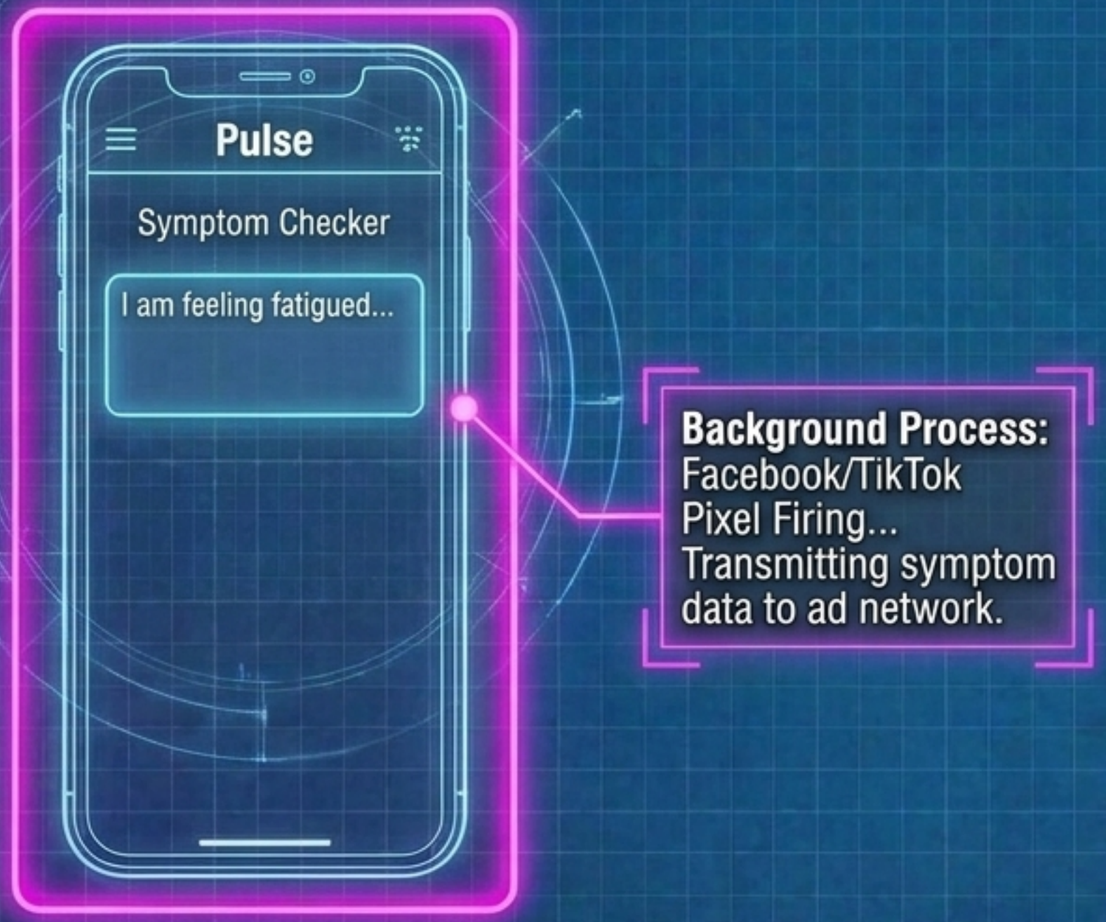
The Trap: Because the app is direct-to-consumer, **HIPAA does not apply**. Instead, it falls under the **FTC's HBNR** (amended July 2024).

A "breach" is not just a hacker stealing data; intentionally sharing health data with unauthorized third parties triggers mandatory FTC and media notifications, **carrying penalties of $51,744 per violation.**

⚠ WARNING

Gemini Notebook

The Ad Pixel Jeopardy



The Chain Reaction

1. User enters symptom (Classified as Consumer Health Data).
2. Marketing pixel fires to ad network (Constitutes a CCPA Sale/Share).
3. Trigger: Violates CA § 1798.121 (Failure to provide Right to Limit).
4. Trigger: Violates CO/VA/CT/TX (Failure to obtain Affirmative Opt-In for sensitive data).
5. Trigger: Constitutes potential unauthorized disclosure under **FTC HBNR**.

WARNING

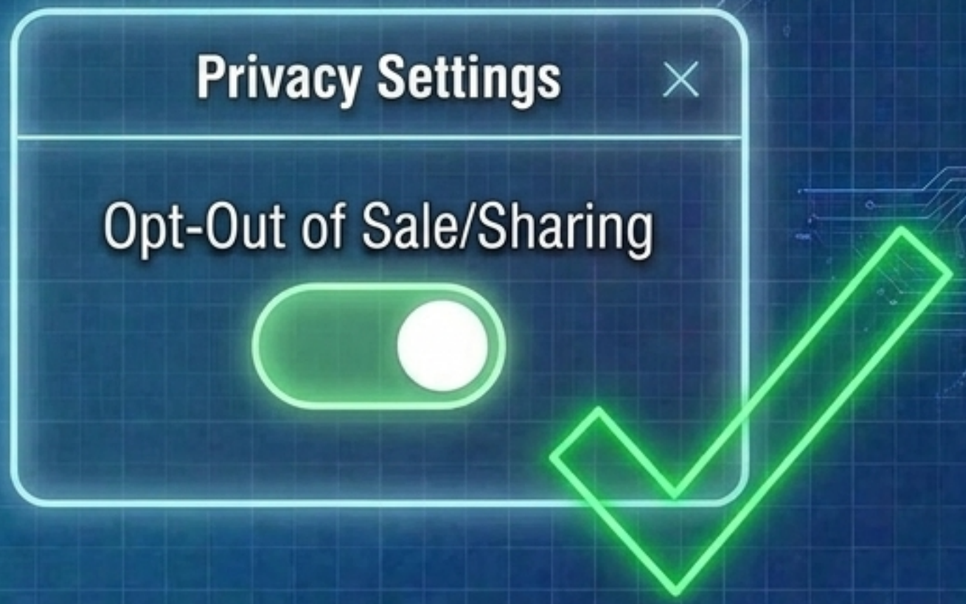
Gemini Notebook

Trap 1: Over-Verifying Identity

Violating UX



Compliant UX



Legal Translation: CPPA Advisory 2024-01 expressly prohibits over-verifying. You cannot ask a user to create an account, provide a government ID, or surrender more personal data simply to opt out. The verification process must adhere strictly to data minimization principles.

WARNING

Gemini Notebook

Trap 2: Dark Patterns & Asymmetry

Asymmetrical / Violating

Cookie/Privacy Banner

ACCEPT ALL

Manage Preferences -> Step 2 -> Step 3

Symmetrical / Compliant

Cookie/Privacy Banner

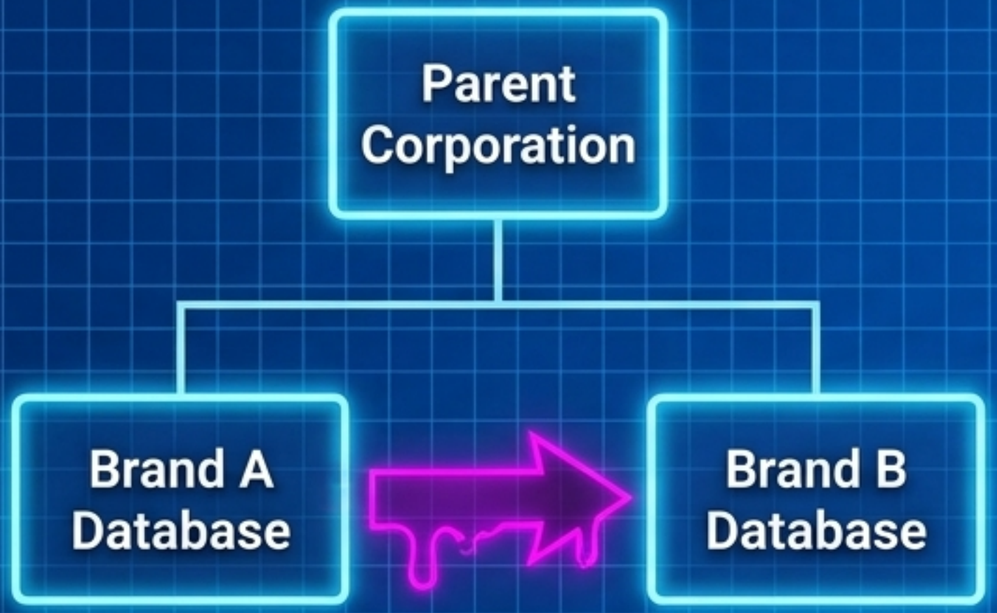
ACCEPT ALL **DECLINE ALL**

CPPA Advisory 2024-02 Rule: Dark patterns are judged by effect, not intent. The path to exercise a privacy-protective option cannot be longer, more difficult, or more time-consuming than the less-protective option. Symmetry in choice is legally mandated.

Gemini Notebook

Trap 3: Corporate Blind Spots & Stealth Edits

Corporate Boundaries



Multi-brand entities cannot freely share opt-outs or data across corporate boundaries without explicit mapping. (CPPA Advisory 2025-01).

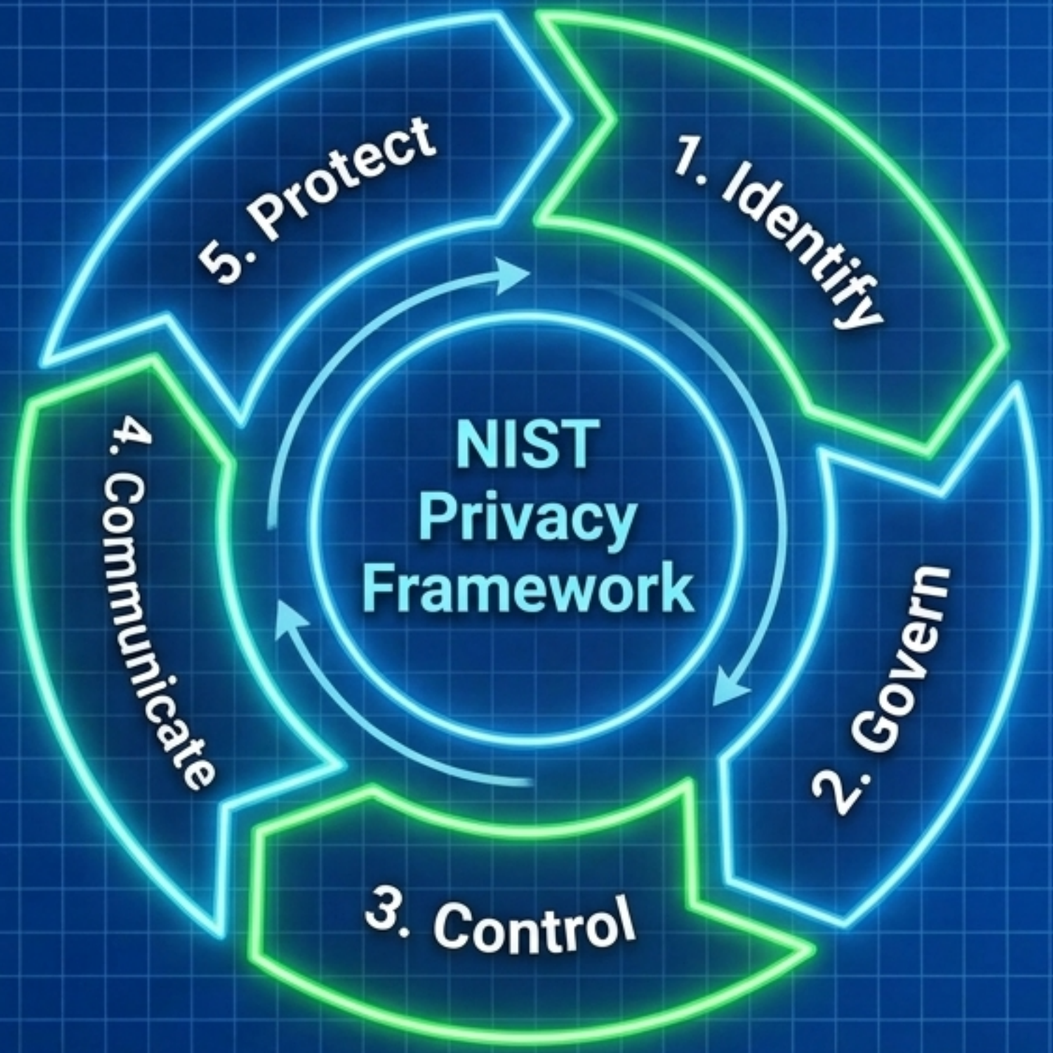
Terms of Service Updates



Quietly editing a ToS agreement to retroactively train AI models on user data without affirmative consent is a heavily monitored FTC Section 5 “Deceptive Practice” red flag.

Gemini Notebook

Unifying Controls: The High-Water-Mark Flow



The Synthesis Insight:

Small teams cannot build 20 different state-specific app variations. The engineering standard is to map to the NIST Privacy Framework and build to the strictest US requirement (the “High-Water-Mark”).

- Build universal upfront opt-ins for sensitive data.
- Implement frictionless GPC support everywhere.
- Map all vendors to strict Service Provider contracts.

Gemini Notebook

Red Lines for Counsel & Wrap

Stop coding and call privacy counsel if:

- [x] Processing data of known under-13s (COPPA applies).
- [x] Handling consumer health, neural, or biometric data (HBNR / CTDPA applies).
- [x] Selling data as a primary business model (Data Broker classification & DROP platform integration).

Next Up



Mandatory Disclaimer: General information, not legal advice — current as of November 2026.

Gemini Notebook