US Biometric Privacy - Compliance Starter

Face recognition is the highest-liability feature in a US surveillance system. Frame it before you procure. Engineering guidance, not legal advice - confirm specifics with qualified counsel.

What is even 'biometric'? The template, not the picture (BIPA Sec. 10)

IN (regulated): a scan of face geometry (a 'faceprint'), a fingerprint, an iris or retina scan, a voiceprint - any template used to identify a person. OUT: photographs, plain video, and physical descriptions (height, hair color). The rule: recording video is fine; building an identity template is the regulated act. Detection ('a face is present') is out; recognition ('this is a specific person') is in.

The US patchwork - who can make you pay

Law	Consent rule	Who enforces	Headline exposure
Illinois BIPA 740 ILCS 14	Written notice + signed release BEFORE capture	Individuals (private right) + class actions	$1,000 / $5,000 per person; fees; injunction
Texas CUBI 503.001	Inform + consent before capture	Attorney General only	Up to $25,000 / violation (Meta: $1.4B, 2024)
Washington RCW 19.375	Notice + consent before DB enrolment	Attorney General only	Consumer Protection Act penalties
~20 states (CA, CO, ...)	Opt-in consent (biometrics = 'sensitive data')	Attorney General (generally no private suit)	Statutory fines per violation

The BIPA consent gate (Sec. 15(b)) - all three, in order, BEFORE capture

(1) Tell the person in writing that a biometric is being collected or stored. (2) Tell them, in writing, the specific purpose and the length of term. (3) Receive a written release they actually sign. In a controlled setting (employees, members) this is workable; for a camera that faceprints everyone who walks past, it is structurally impossible - you cannot get a stranger's signature in advance. Also keep a public retention policy and destroy biometrics when the purpose ends or within 3 years (Sec. 15(a)); never sell or profit from them (15(c)).

Why Illinois is the dangerous one - the per-person math

Illinois alone lets the people in your footage sue you, and Rosenbach v. Six Flags (2019) says they need prove NO harm - the violation is the injury. Damages are fixed: $1,000 (negligent) or $5,000 (reckless) PER PERSON. Face-recognition on 50,000 shoppers with no release = $50M (negligent) to $250M (reckless), before fees. The 2024 amendment (SB 2979) caps this at one recovery per person (not one-per-scan) - but the per-person multiplier stands. Real results: Facebook $650M; Texas-Meta $1.4B; Clearview ~$51.75M equity.

Run before you procure

[ ] Map where your pipeline builds an identity template (faceprint / voiceprint). [ ] Biometric analytics OFF by default; enabling it is a documented decision. [ ] Where you cannot get consent, do NOT build the template - detect/count only. [ ] Written-release + notice flow in place wherever you do build one. [ ] Geo-fence biometric capture to consent-enabled sites (disable in Illinois without a flow). [ ] Retention/destruction clock set (BIPA <= 3 yr; Texas <= 1 yr). [ ] Build-vs-buy: the vendor's biometric feature is YOUR liability once enabled.

This is engineering guidance, not legal advice. The definitions, consent gate, damages, and the 2024 single-recovery amendment are summarised for planning - the BIPA damages doctrine is still moving in the courts; confirm the current specifics for your states with qualified counsel. There is no comprehensive federal biometric law; state rules govern.