Part 5: Security & Critical Thinking

Scenario 1:

You’re asked to store face scan data locally for a future feature. Your manager insists it's "just temporary" and asks you to write it to disk in base64.

Legal concerns:

- GDPR / CCPA / other privacy laws treat biometric data as sensitive personal information.
- Storing unencrypted biometric data (even base64) may violate compliance and expose company to legal risk.

Ethical concerns:

- Biometric data is non-revocable — a leak is irreversible for the user.
- Temporary storage tends to become permanent without proper controls.

Architectural concerns:

- Base64 is not encryption, just encoding.
- Writing raw sensitive data to disk without encryption or sandbox restrictions opens the door to data breaches.

Secure design proposal:

- Store only encrypted data, using Keychain or Secure Enclave when available.
- Avoid writing raw biometric data to disk altogether.

Scenario 2:

You’re told to sync user data via Firebase and also store it in plaintext in Core Data “to make debugging easier.” How do you respond?

- Propose using obfuscated test data or mock environments for debugging.
- If real data is required, encrypt fields in Core Data using a lightweight encryption layer (e.g. AES + Keychain-stored key).
- Ensure logs/debug outputs never expose Personal Info.