Lewis Joseph Feik
Case project 6-2
Security Awarness

Smartphone Privacy Rules in 2025: Where We Are and What Should Change

*Policymakers on both sides of the Atlantic have tightened rules that shape how Apple and Google design smartphones and how advertisers can use user data. In the EU, two flagship laws dominate: the **Digital Markets Act (DMA)**, which compels "gatekeepers" to open up platforms and curb self-preferencing, and the **Digital Services Act (DSA)**, which polices systemic risks such as scams and opaque targeting. The European Commission opened non-compliance probes into Apple and Alphabet in March 2024 and, in 2025, issued preliminary findings signaling violations; the DSA is also being used to demand information from Apple and Google about combating online scams. Digital Markets Act (DMA)+2The Register+2*

*Enforcement has teeth. In March 2025, France's competition regulator fined Apple **€150 million** over how its App Tracking Transparency (ATT) framework was implemented, finding it could disadvantage third parties. Whether or not one agrees with the theory, the case underscores that authorities are willing to penalize privacy designs if they entrench market power or create unequal consent flows. Separately, Apple has warned that DMA-driven changes are delaying or altering EU features, highlighting a real tension: opening platforms for competition can collide with platform-level privacy/security controls. Autorité de la Concurrence+1*

*In the U.S., there is still no comprehensive federal privacy statute. Instead, the **California Consumer Privacy Act** as amended by the **CPRA** sets a de facto baseline: people may opt out not only of "sales" of data but also of **sharing for cross-context behavioral advertising** (surveillance-based ads), and companies must honor those choices. Other states have similar laws, but protections vary. At the federal level, the **FTC** opened a rulemaking on "commercial surveillance and data security" that remains active, signaling possible rules around data minimization and consent, though a final rule has not landed. In short, U.S. coverage is improving piecemeal, but remains patchy and uneven across states. National Law Review+3California DOJ AG Office+3California Lawyers Association+3*

*Meanwhile, the ad-tech stack is shifting. Google's **Privacy Sandbox** on Android replaces persistent identifiers (like MAIDs) with APIs for attribution and targeting intended to reduce cross-app tracking; yet on the web, Google paused cookie deprecation and scaled back Sandbox plans after pushback from regulators and industry raising hard questions about whether the "privacy preserving" alternatives meaningfully curb surveillance or simply reshuffle it. The picture is that technical privacy mitigations are arriving, but their effectiveness and competitive effects are under scrutiny. Google Help+2INCRMNTAL+2*

Lewis Joseph Feik
Case project 6-2
Security Awarness

Are current rules adequate? *Partly. The EU's DMA/DSA pairing and targeted enforcement give regulators real leverage over platform defaults and opaque ad practices. In the U.S., state laws (especially CPRA) meaningfully expand consumer rights—but the mosaic leaves gaps users can't easily navigate, and enforcement resources are finite. Across jurisdictions, three problems persist: (1)* ***opaque data flows*** *between apps, SDKs, and brokers; (2)* ***consent fatigue*** *that nudges users toward surveillance by design; and (3)* ***market-power dynamics*** *where privacy changes may double as competitive levers, complicating remedies. Recent Apple enforcement and DMA probes demonstrate that privacy and competition are now intertwined—and that design choices can either reinforce or reduce tracking at scale. Autorité de la Concurrence+2Digital Markets Act (DMA)+2*

What should be done?

1. ***Make opt-outs universal and automatic.*** *Require operating systems to honor a standardized device level opt-out (or opt-in by default for targeted ads) across all apps and ad SDKs, enforceable via platform audits and fines. This would generalize CPRA-style choices beyond state boundaries. California DOJ AG Office*

2. ***Mandate data-minimization APIs by default.*** *Build on Android's Sandbox idea but require independent audits showing that new APIs actually reduce cross-app/linkable identifiers versus status quo, with sunset clauses for legacy identifiers. Google Help+1*

3. ***Require standardized transparency for data flows.*** *Both app stores should compel SDK "nutrition labels" that list recipients, retention periods, and lawful bases, with machine-readable disclosures regulators can crawl. Tie label accuracy to meaningful penalties under competition and consumer-protection law. Digital Markets Act (DMA)*

4. ***Strengthen cross-regime coordination.*** *Encourage joint privacy-and-competition enforcement (as in the French ATT case and EU DMA probes) to prevent privacy features from being weaponized competitively or, conversely, to ensure "openness" doesn't expand tracking. Autorité de la Concurrence+1*

5. ***Advance a U.S. federal baseline.*** *An interoperable federal law should guarantee opt-out (ideally opt-in for minors), data minimization, sensitive-data limits (including precise location), and a private right of action while letting states go further. If FTC rulemaking lands first, it should target dark patterns, secondary uses without consent, and brokered location data. Federal Trade Commission*

Bottom line: *Today's laws are finally pressuring Apple, Google, and the ad ecosystem but they are not yet a full answer to surveillance based business models. Making privacy* ***the default****, verifying it with* ***audits and enforcement****, and aligning competition and privacy goals will do more to protect users than any one consent screen ever could*