**PETITION FOR RULE MAKING**
California Administrative Procedure Act (Gov. Code § 11340. )

**California Administrative Procedure Act (Gov. Code § 11340.6)**Petition for Rulemaking Regarding Tiered Consent and Minimal Functional Mode for Essential Consumer Devices

| | |
|---|---|
| **Submitted to:** | **California Privacy Protection Agency** |
| **Petitioner:** | [redacted] |
| **Contact:** | [redacted] |
| | [redacted] |
| **Date:** | 02/09/2026 |

## I. EXECUTIVE SUMMARY

This Petition formally requests that the California Privacy Protection Agency (hereinafter "CPPA" or "the Agency") initiate rulemaking proceedings to articulate and enforce the California Privacy Rights Act's (hereinafter "CPRA") mandates concerning data minimization, purpose limitation, and the requirement of voluntary, meaningful consent within the context of essential consumer devices, specifically general-purpose consumer devices such as smartphones, laptops, wearables.

Current industry practice obligates consumers to consent to comprehensive Terms and Conditions, which govern a wide array of non-essential data processing activities, as an indispensable precondition to accessing even fundamental and safety-critical device functions, including, but not limited to, emergency calling, basic telephony, messaging services, and offline utilities and general internet access. This Petition proposes the adoption of a regulatory framework that mandates the establishment of a **Minimal Functional Mode** and a **tiered consent structure** to ensure that consumer consent is proportional, freely given, and fully compliant with the core principles of the CPRA.

## II. STATUTORY AUTHORITY

The CPPA possesses clear and explicit authority, pursuant to the CPRA, to promulgate regulations designed to further the principles of privacy-by-design, data minimization, purpose limitation, and proportional consent. The Agency is specifically empowered to clarify the standard for what constitutes meaningful consent and to define the scope of data processing that is genuinely necessary within specific technological contexts, such as device activation workflows.

Furthermore, the CPRA mandates heightened privacy protections for minor consumers, thereby underscoring the imperative for regulatory action to enforce privacy-protective defaults and implement safeguards against coercive consent mechanisms.

## III. BACKGROUND AND CURRENT PRACTICES

Contemporary consumer devices, particularly smartphones or laptops, are engineered such that users must accept a singular, expansive Terms and Conditions agreement prior to being granted access to any meaningful functionality. A refusal to accept these terms renders the device substantially inoperable, preventing the user from executing fundamental actions such as placing calls, transmitting messages, accessing emergency services, or utilizing core offline applications.

These agreements routinely encompass and govern data practices that are entirely ancillary to the basic, necessary operation of the device, including, but not limited to, the provision of cloud services, the collection of performance analytics, telemetry data capture, and stipulations regarding mandatory arbitration.

## IV. CPRA IMPLICATIONS

The practice of conditioning access to essential device functionality upon the acceptance of non-essential data processing practices constitutes a direct contravention of core CPRA principles. Consent obtained under duress or necessity cannot, by definition, be considered voluntary, informed, or freely given. Given that basic device functions can demonstrably operate without reliance on extensive cloud services or superfluous telemetry, the current scope of data collection is rendered disproportionate to the stated purpose.

The highly concentrated nature of the consumer device market further diminishes effective consumer choice, significantly exacerbating the coercive nature inherent in the current practice of bundled consent at the point of device activation.

## V. PROPOSED REGULATORY FRAMEWORK

### A. Core Functional Mode

The Agency should mandate a **Core Functional Mode** for all general-purpose consumer devices. This mode ensures that a device is "functional out-of-the-box" for its primary purpose without requiring the user to link a persistent cloud identity or consent to ancillary data collection.

- **Definition**: A state of operation that enables all hardware-level features (e.g., camera, local file storage, basic telephony, and local utilities) that are technically capable of functioning without cloud-based processing.
- **Scope of Access**: Users must be able to skip "Account Creation" or "Cloud Terms" while retaining access to the basic browser, messaging, and local applications.
- **Data Minimization**: Within this mode, only data strictly necessary for the immediate, user-initiated task may be processed (e.g., processing a photo locally on the device rather than syncing it to a cloud server).

### B. Tiered Consent Structure

Functionality beyond the Core Functional Mode shall be enabled only through a progressive, contextual, and distinct consent mechanism. This ensures consent is **voluntary and proportional** to the benefit received.

| Tier | Description | Requirement | Default Status |
|---|---|---|---|
| **Tier 1** | **Core Functional Mode** | Essential telephony, local apps, and basic hardware use. | **Always Enabled** |
| **Tier 2** | **Enhanced Services** | Opt-in features requiring a cloud account (e.g., cross-device syncing, find-my-phone). | **Disabled by Default** |
| **Tier 3** | **Ancillary Processing** | Analytics, telemetry, and personalization for marketing/ad-profiling. | **Disabled by Default** |

Users shall have the continuing right to modify their consent preferences at any time, including the right to reduce, withdraw, or expand previously granted consent, without obligation to maintain prior consent selections. Such modification should not result in denial of core device functionality beyond what is strictly necessary for the requested service.

### C. Prohibition of Bundled/Coercive Consent

- **Decoupling**: Manufacturers are prohibited from conditioning the use of Tier 1 (Core) functions on the acceptance of Tier 2 or Tier 3 data processing.
- **Transparency**: Consent for Tier 2 and Tier 3 must be requested contextually—at the time the user attempts to use an enhanced feature—rather than being buried in a singular, all-or-nothing activation workflow.

## VI. TECHNICAL FEASIBILITY AND PRECEDENTS

The implementation of a **Core Functional Mode** and **Tiered Consent** does not require the invention of new technology; rather, it mandates the standardization of existing architectural patterns found in modern computing and web services.

### A. Precedent in Web Standards: The "Essential" vs. "Non-Essential" Tiering

The most prominent technical precedent for this framework is the **Standardized Cookie Classification** used globally under the GDPR and ePrivacy Directive.

- **Tiered Logic**: Modern web architecture already distinguishes between **"Strictly Necessary"** cookies (essential for security and core site functions) and **"Targeting/Analytics"** cookies.
- **Implementation**: This logic can be directly mapped to hardware. A device's "Strictly Necessary" tier would include local OS functions and hardware drivers, which—like essential cookies—should be enabled by default and exempt from opt-in requirements to ensure immediate utility.

### B. Precedent in Mobile Architecture: Functional Decoupling

Technical research, such as the **CURLED (Consent reqUests foR mobiLE Devices) Framework**, demonstrates that "functionality-based" consent is highly effective and technically achievable.

- **System-Level Isolation**: Modern mobile operating systems (iOS and Android) utilize **Sandboxing** and **Trusted Execution Environments (TEEs)** to isolate core processes from cloud-linked analytics.
- **Proven Efficacy**: The CURLED research shows that users can successfully navigate "Tiered Consent" when it is tied to specific functionalities rather than "Accept All" bundles. This proves that the binary, all-or-nothing activation workflows currently used by manufacturers are a choice of business model, not a technical necessity.

### C. Precedent in Privacy Signals: Automated Enforcement

The CPPA has already established a technical precedent by requiring businesses to honor the **Global Privacy Control (GPC)**.

- **Scaling to Hardware**: Just as the GPC allows a browser to communicate a user's "Do Not Track" preference automatically, a device's **Core Functional Mode** would act as a hardware-level privacy signal. It ensures that the "Skip Account Sign-In" action serves as a universal opt-out for all Tier 2 and Tier 3 data processing, as technically defined by the W3C's Tracking Preference Expression.

### D. Precedent in Corporate Compliance: Data Minimization Mandates

Existing enterprise standards (e.g., **NIST SP 800-124**) already recommend that mobile devices be secured by limiting unnecessary connections and disabling non-essential functionality. By mandating these standards for all consumers, the Agency would simply be extending "best-practice" enterprise security and privacy to the general public.

## VII. PUBLIC BENEFITS

The adoption of the proposed framework would yield significant public benefits, including a material enhancement of consumer privacy protections, guaranteed access to safety-critical and basic functionality without privacy sacrifice, robust protections for minors, an increase in consumer trust in device manufacturers, and the provision of essential regulatory clarity for industry stakeholders.

## VIII. REQUESTED AGENCY ACTION

The Petitioner respectfully requests that the CPPA formally initiate rulemaking proceedings to achieve the following: (1) define and require the implementation of a Minimal Functional Mode; (2) mandate a tiered consent structure for consumer device activation; and (3) solicit public input through structured workshops or formal comment processes.

# IX. CONCLUSION AND REQUEST FOR ACTION

For the reasons set forth above, the current "all-or-nothing" device activation models prevalent in the consumer technology market create a coercive environment that is fundamentally incompatible with the CPRA's mandates for data minimization and voluntary consent. By conditioning the basic utility of essential devices on the acceptance of broad, non-essential data processing, manufacturers are undermining the foundational privacy rights of California consumers.

The Petitioner respectfully requests that the California Privacy Protection Agency exercise its statutory authority to initiate formal rulemaking to establish a **Device Functional Integrity Standard**. Specifically, the Petitioner requests that the Agency:

1. **Define and Mandate a "Core Functional Mode"**: Require that all general-purpose consumer devices (smartphones, laptops, and wearables) enable basic hardware and software functionality—including telephony, local applications, and essential security—without requiring a user to link a cloud identity or consent to non-essential data collection.
2. **Codify a "Tiered Consent" Framework**: Establish a mandatory regulatory structure where device activation is decoupled from secondary data processing. Manufacturers must be required to obtain distinct, contextual consent for enhanced cloud services (Tier 2) and ancillary analytics or marketing (Tier 3), with these features being disabled by default.
3. **Prohibit Bundled and Coercive Activation Workflows**: Formalize a standard that prohibits manufacturers from holding "Tier 1" core functionality hostage to the acceptance of broad terms governing non-essential data practices.
4. **Establish Privacy-by-Default for Minors**: Implement heightened technical safeguards that mandate the Core Functional Mode as the default state for all devices identified as being used by minors, ensuring their immediate safety and communication needs are met without compromising their long-term digital privacy.

The proposed framework is technically feasible, aligns with established web standards for "essential" cookies, and directly fulfills the Agency's mission to protect the privacy of Californians in an increasingly connected world.

Respectfully submitted,

[redacted] *Petitioner* Dated: February 9, 2026

**APPENDIX A – MINORS, YOUTH SAFETY, AND MEANINGFUL CONSENT**

The CPRA explicitly recognizes that minor consumers are entitled to heightened privacy safeguards. Device activation workflows that compel the acceptance of non-essential data practices as a requisite for accessing critical emergency and communication functions place minors in an unacceptable dilemma between personal privacy and immediate safety.

A Minimal Functional Mode would establish mandatory, privacy-protective defaults for youth users, while simultaneously preserving the ability for parents and legal guardians to incrementally enable additional services through explicit consent, thereby remaining consistent with the foundational intent of the CPRA.