Documentation was prepared with the assistance of AI-based tools, used responsibly for drafting support and consistency checks.
The core conceptual framework was finalized in 2024, followed by the completion of the AI implementation in 2025.
The resulting AI system remains intentionally lightweight—under 200KB—allowing for secure and practical distribution via Bluetooth in low-connectivity environments.

The framework is explicitly white-box by design, ensuring full transparency and verifiability, with no reliance on probabilistic inference that could produce AI hallucinations.

This design is not intended to neutralize inspections or evade authorities. Rather, it is a pragmatic survival-oriented approach aimed at reducing unnecessary suspicion during the earliest stages of device checks.

1. Application of Tradecraft: Beyond Software, Into Survival

- **The Problem (The "Flagging" Risk):** Standard security tools like Signal, Tor, or encrypted vaults inadvertently act as a "digital flag." In high-risk zones like Myanmar or Iran, the mere presence of these apps during a physical device search signals to authorities: *"I am an activist."* This exposes the user to immediate interrogation or arrest before they can even use the tool.
- **Our Solution (Plausible Deniability):** We apply the principle of **"Digital Tradecraft."** VitalGuard is fully camouflaged as a functioning **Calorie Management App**. It provides a perfect cover story ("I am managing my health/diabetes"), effectively neutralizing suspicion during visual inspections.
- **The Survival Trigger:** We utilize the innocuous word **"Diet"** as a panic trigger. Unlike a panic button which requires physical interaction, this voice-activated trigger fits naturally into the app's context while acting as a "kill switch." This is not just a feature; it is a **survival mechanism** designed for the reality of physical coercion, where users may be handcuffed or unable to touch their screens.

2. Technical Counter-Intuition: Cryptographic Erasure over Overwriting

- **The Failure of Tradition:** Traditional security protocols rely on "Data Overwriting" (e.g., DoD standards). However, on modern smartphones

using Flash Memory (SSD/eMMC), **wear-leveling algorithms** make guaranteed physical overwriting practically impossible. Residual data often remains in spare blocks, vulnerable to forensic recovery.

- **Our Innovation (Key Destruction):** We implement **"Cryptographic Erasure"**—a method superior to physical deletion.
    1. All sensitive data is encrypted at rest (AES-256).
    2. The decryption keys are stored **only in volatile RAM**, never written to disk.
    3. Upon triggering, we do not waste time trying to overwrite gigabytes of data. Instead, we **instantly wipe the encryption keys from RAM**.
- **The Result:** The data remains on the device but is instantly transformed into **high-entropy cryptographic noise**, mathematically impossible to recover without the keys. This is the **only technical approach** capable of achieving total data sanitization in under **0.01 seconds**—the critical window during a surprise raid.

Ethical philosophy cannot be replicated by coding skills alone.

Life-saving technology is not defined by the complexity of its code, but by the ethical principles that guide its design and deployment.

In high-risk and rights-restricted environments, technical sophistication alone does not protect users. What ultimately determines whether a system preserves life and dignity is a clear ethical philosophy—one that prioritizes human rights, minimizes harm, and respects user autonomy under real-world constraints.

This project is therefore built on the premise that responsible AI for internet freedom must begin with ethics-first architecture. Technical decisions, including minimalism, offline operation, and zero-trace design, are direct consequences of this philosophy, not afterthoughts. The goal is not to demonstrate technical excess, but to deliver technology that can be trusted by those whose lives may depend on it.