Last updated: May 04 2025

1. Introduction

TunnelSight (“we,” “us,” or “our”) is committed to protecting your privacy. TunnelSight is an on-device packet-inspection tool for iOS that gives you real-time visibility into HTTP/HTTPS traffic generated by your own device. This Privacy Policy explains what information the app processes, how it is used, and what control you have over that data.

By installing and using TunnelSight, you agree to the terms of this Privacy Policy.

2. Data Processed On-Device Only

- **All packet capture, decryption, inspection, storage and analysis occurs entirely on your iPhone or iPad.**
- We do **not** transmit, upload or share any intercepted request, response, header or body data to any server—yours or ours.
- When you export data (cURL, JSON), the resulting file remains on your device until you explicitly share it (e.g. via Mail, Files, AirDrop).

3. Types of Data

TunnelSight may read or store the following data **locally** on your device:

Data Type	Purpose	Shared Off-Device?
HTTP(S) headers (request & response)	Inspection, debugging	No
HTTP(S) payloads (bodies)	Raw-data viewing, JSON export	No
Timestamps, URLs, methods, status codes	Session history, search/filter	No
cURL commands & JSON exports	User-initiated sharing	Only when you choose to export/share

4. Device Identifiers & Certificates

- TunnelSight generates a **unique, per-device, self-signed root-CA certificate** to decrypt HTTPS traffic.
- The certificate’s private key is stored in the iOS Secure Enclave–backed keychain.
- Certificate and key remain on your device; they are never backed up or transmitted elsewhere.

- You can remove the certificate at any time via Settings → General → VPN & Device Management.

5. Third-Party SDKs & Services

TunnelSight does **not** include any third-party analytics, advertising, or crash-reporting SDKs. We rely solely on Apple's public APIs (NetworkExtension, CryptoKit, Configuration Profiles, NIO).

6. Your Controls

- **Persistence toggle**: In Settings, you can choose whether captured sessions persist across app restarts.
- **Clear data**: Tap "Clear All" in-app to delete all captured packets from memory and disk.
- **Remove certificate**: Uninstall the root-CA profile at any time via iOS Settings.
- **Export/share**: You decide if and when to export or share any data.

7. Data Retention

- If "Persistence" is **off**, all captured data is purged automatically when you background or terminate the app.
- If "Persistence" is **on**, data remains on-device until you manually clear it.

8. Children's Privacy

TunnelSight is a developer tool not intended for children under 17. We do not knowingly collect information from minors.

9. Security

We implement industry-standard measures to secure data on your device, including:

- Encryption of stored data using iOS file-protection APIs.
- Secure Enclave storage for private keys.
- No external network connections for captured data.

10. Changes to This Policy

We may update this Privacy Policy from time to time. If we make material changes, we will update the "Last updated" date. Continued use after changes constitutes acceptance.

11. Contact Us

If you have questions or concerns about this Privacy Policy, please contact us at:
Email: zaknc@icloud.com
Address: Hill Croft, Wonersh Common, GU5 0PH, Guildford, Surrey, United Kingdom

By clicking “Get” or installing TunnelSight, you acknowledge that you’ve read and understood this Privacy Policy.