GLACIER · TECHNICAL WHITEPAPER

Privacy, security, and transparency on Android.

The privacy and security controls implemented in Glacier for Android.

EDITION	VERSION	PUBLISHED	SOURCE BASIS
Customer	1.1	20 October 2026	`b2652cd · 04befc6`

Published by Glacier for customers, partners, security teams, and privacy reviewers

OUR COMMITMENT

Privacy protection is built into the Android product

Glacier encrypts protected network paths, applies filtered DNS, checks selected device conditions locally, limits sensitive configuration storage, and offers a separate Glacier number for supported calls.

EXECUTIVE SUMMARY

Android protection works in layers

Glacier for Android provides two protection modes through Android VpnService. Standard Protection carries encrypted DNS through WireGuard while ordinary app traffic stays on its normal path. Extra Protection carries supported IPv4 traffic and DNS through the Glacier WireGuard gateway. Both modes use the signed-in account's managed DNS profile.

The app also provides an on-device Security Hub, encrypted storage for WireGuard configuration, app-private call records, an application manifest that disables automatic backup, optional screen-capture blocking, authenticated service requests, and an optional Glacier phone number. Glacier's backend uses pseudonymous account identifiers for managed DNS and calling resources.

Four protection layers

01

Network protection

Extra Protection encrypts supported IPv4 traffic to the selected Glacier gateway. Standard Protection limits the tunnel to DNS traffic.

02

Protected DNS

Both modes use profile-attributed DNS-over-TLS. Standard resolves on the device through WireGuard. Extra uses either the same path or a gateway-forwarded path that is enabled only by an explicit profile marker.

03

Device visibility

The Security Hub checks release authenticity, debug state, root and hook indicators, proxy settings, USB debugging, screen lock, biometrics, version currency, and live protection health.

04

Private calling

A Glacier number reduces disclosure of the customer's personal number. Current backend provisioning uses one random account UUID for Twilio number ownership, access tokens, and client routing.

SECURITY REVIEW UPDATES

Tighter delivery, storage, and authentication paths

Recent Android changes constrain VPN profile downloads, pin Glacier service connections to Amazon root certificate authorities, disable HTTP body logging in release builds, tighten authentication and purchase ownership decisions, make account exit clear local state even when the network is unavailable, and add scheduled vulnerability scanning for the native and JVM dependency sets.

01 ABOUT THIS PAPER

How we substantiate each statement

We prepared this edition from Glacier Android source revision `b2652cd` as of 4 September 2026. The backend sections use the same reviewed Console source revision `04befc6` and the same policy basis as the iOS whitepaper. Public protocol, Android, and provider documentation supports

statements about platform and transport behavior.

The evidence label matters. A source-verified control is implemented in the reviewed code. A Glacier policy commitment states how the company says it handles production data. A provider-documented behavior describes a service boundary that Glacier does not operate.

EVIDENCE LABEL	WHAT THE LABEL MEANS	REPRESENTATIVE USE
Source-verified control	Implemented in the cited Android or Console source revision.	VpnService routing, encrypted profile storage, authorization checks, and local cleanup.
Glacier policy commitment	A current published Glacier commitment for production data handling.	No itemized VPN or DNS activity logs, no advertising trackers, and privacy request handling.
Provider-documented behavior	A platform, protocol, or provider property described by its operator.	Android VpnService behavior, WireGuard cryptography, and Twilio TLS and SRTP transport.

Table 1. Evidence labels used throughout this paper.

Scope and currency

- This paper covers Android permissions, local storage, authentication, DNS and VPN operation, calling, backend privacy controls, published policies, and vulnerability reporting.
- Source review establishes implemented controls. It does not certify a particular production deployment, credential rotation event, or provider operation.
- Customers should use the latest supported Android build and the current Privacy Policy for current product and processing terms.

02 ARCHITECTURE AND TRUST MODEL

Purpose-specific paths limit data exposure

Glacier separates protected DNS, full VPN traffic, authenticated app APIs, calling, and local records. The Android device keeps account-scoped preferences, an app-private database, and an encrypted WireGuard configuration. Glacier services handle authenticated account operations. The managed resolver handles filtered name resolution, the VPN gateway handles tunneled traffic, and Twilio handles calls when the phone feature is used.

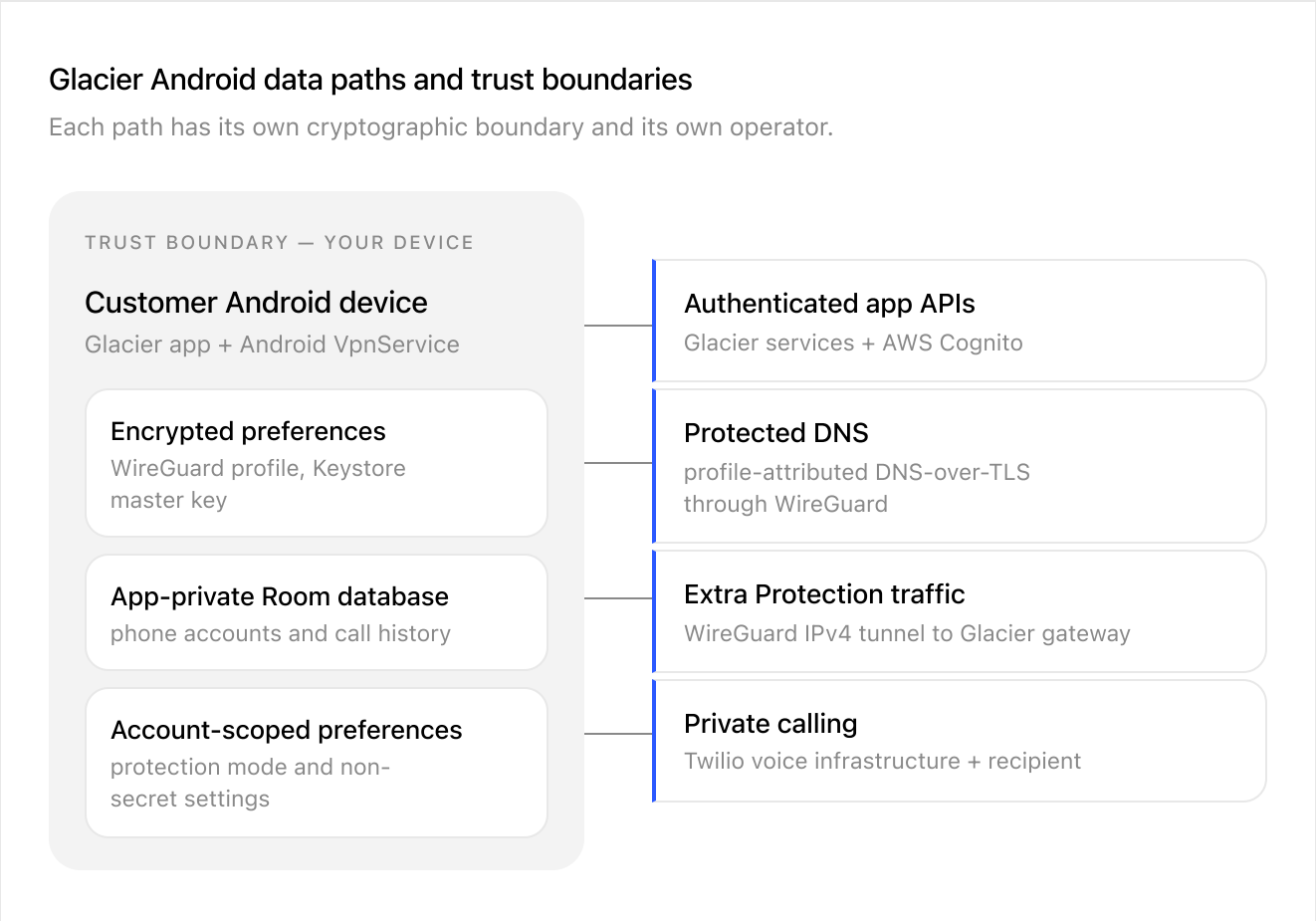


Figure 1. Android protection uses separate network, account, calling, and local storage paths.

Primary data paths

PATH	IMPLEMENTED PROTECTION	PRIMARY ENDPOINT	EVIDENCE
Extra Protection traffic	WireGuard over Android VpnService with IPv4 default routing	Glacier VPN gateway	Source-verified control plus WireGuard documentation
Standard Protection DNS	DNS-over-TLS through WireGuard; ordinary traffic bypasses	Managed DNS service	Source-verified control plus RFC 7858
App and account APIs	Bearer authentication, bounded requests, and CA public-key pinning	Glacier services and AWS Cognito	Source-verified control
Voice calling	Glacier number, UUID account identity, TLS signalling, and SRTP media	Twilio and telephone network	Backend control plus provider documentation
Local records	App-private Room database, backup disabled, encrypted VPN profile store	Android device	Source-verified control plus Android documentation

Table 2. Data paths, their implemented protection, and the evidence behind each.

03 PROTECTION GOALS

The exposures Glacier is designed to reduce

Glacier addresses untrusted access networks, routine DNS observation, classified tracker and malicious domains, weak device settings, tampered app environments, unnecessary provider identifiers, and disclosure of a personal phone number.

GOAL	CONTROL	CUSTOMER RESULT
Reduce access-network visibility	Extra Protection sends supported IPv4 traffic through WireGuard.	The access network sees encrypted tunnel traffic; ordinary destinations see the gateway address.
Protect DNS	Standard and Extra use profile-attributed DNS-over-TLS carried by WireGuard.	The local network does not receive the customer's resolver exchange in plaintext.
Block classified domains	The managed DNS profile applies security and privacy filtering.	Matching domains are blocked under the active provider profile.
Surface device risks	The Security Hub reports Android, app, proxy, debug, integrity, and protection signals.	Customers receive local checks with confidence and unknown states kept distinct.
Reduce calling identity exposure	A Glacier number replaces the personal number for supported calls; routine provider resources use an account UUID.	Recipients do not receive the customer's personal number from the Glacier calling flow.
Limit stored network secrets	The WireGuard profile is stored in encrypted preferences backed by a MasterKey.	Tunnel private key material is not written as ordinary plaintext preferences.

Table 3. Each protection goal, the control that addresses it, and the customer result.

Safeguards that still matter

Glacier works alongside a current Android release, a strong screen lock, HTTPS, secure account credentials, and careful handling of links and content. A VPN cannot control information a customer sends directly to a destination, and local protections cannot secure an already unlocked and compromised device.

04 NETWORK PRIVACY

WireGuard transport to the gateway

Glacier implements its tunnel through Android VpnService and WireGuard. Android requires the customer to grant VPN consent before the app can establish the protected interface. The service is declared with `BIND_VPN_SERVICE` so the Android system, rather than another app, controls the binding. [S2] WireGuard uses modern authenticated encryption and key agreement. [S5]

Two protection modes

Standard Protection routes only Glacier's synthetic DNS endpoints into the service and lets ordinary application traffic bypass it. The resolver exchange travels through WireGuard. Extra Protection installs the IPv4 default route so supported traffic uses WireGuard as a full VPN.

Extra Protection currently removes inner IPv6 addresses, DNS entries, and routes when the selected gateway has not established verified IPv6 support. Android then blocks IPv6 for that full-VPN session instead of allowing it to bypass the tunnel.

Provisioning and profile controls

- The app prepares backend, resolver, and WireGuard inputs before replacing a usable tunnel.
- VPN configuration requests use the authenticated Glacier API. The backend checks active entitlement and limits compatibility download links to 120 seconds.
- Profile downloads require HTTPS, an allowed AWS or Glacier domain, Amazon root CA pinning, redirect checks on every hop, a 60-second overall deadline, a 64 KiB size limit, and required WireGuard sections before storage.
- The app stores the profile and selected region in encrypted preferences and never logs the profile body, which contains private key material.
- Sign-out stops the active tunnel, clears the encrypted profile and account-scoped settings, and resets runtime state even if another cleanup step fails.
- Backend account deletion revokes WireGuard peers and removes related profile objects before destructive finalization completes.

What each mode changes

With Extra Protection, the local Wi-Fi or Internet access provider sees encrypted WireGuard traffic instead of the supported IPv4 destinations inside the tunnel. Ordinary destinations see the Glacier gateway address. Standard Protection changes the DNS path only, so ordinary traffic keeps its normal source address and continues to rely on HTTPS for content protection.

OUR PRIVACY COMMITMENT

No itemized VPN activity logs

Glacier's Privacy Policy states that the company does not store, retain, or archive itemized VPN activity logs, including destinations, source IP addresses, timestamps, bandwidth, or session records. This is a Glacier policy commitment. [S1]

05 DNS PRIVACY AND FILTERING

Encrypted DNS inside the protected path

Both Android protection modes use the signed-in account's managed resolver profile. Standard Protection performs DNS-over-TLS on the device and carries that connection through WireGuard. Unmarked Extra profiles use the same design while the full IPv4 route is active. [S6]

A marked Extra profile may use stock WireGuard. In that path, ordinary DNS exists only inside the encrypted WireGuard tunnel, and the Glacier gateway sends the request upstream over profile-attributed DNS-over-TLS. The app selects this path only when the downloaded profile contains the exact gateway-DNS marker and passes private-address and route checks.

Account binding and fail-closed behavior

The app fetches the current account's resolver profile before establishing the tunnel. It caches the profile ID and bootstrap addresses for that account, pairs cached addresses with their profile, and clears both on sign-out. A refusal or temporary network failure may use that account's last valid cache. With no usable profile or bootstrap address, Glacier does not create an unfiltered fallback tunnel.

The backend assigns a random UUIDv4 account ID for provider-facing profile names and issues a signed profile only for a device record owned by the authenticated account. Controlled migration tooling can rename legacy email-named profiles while preserving their settings.

Activity minimization and reporting

The reviewed backend provisions managed DNS profiles with security and privacy filtering. The reviewed default instructs the provider to drop the source IP and queried-domain fields. Glacier retrieves numeric totals such as all queries and blocked queries for customer-facing protection statistics.

Glacier's Privacy Policy states that the company does not store, retain, or archive DNS activity logs, including query content, resolver activity, IP addresses, timestamps, or other personally identifiable network activity. Aggregate numeric totals are the stated exception. This is a Glacier policy commitment. [S1]

Health checks and recovery

Glacier checks the active packet engine, WireGuard state, DNS responses, and tunnel data path. Extra Protection also uses independent HTTPS canaries to detect a tunnel-only integrity failure. Recovery is bounded and throttled. An unavailable check remains unknown instead of being reported as a pass.

06 DEVICE SECURITY POSTURE

Security Hub uses local evidence

The Security Hub turns Android and app signals into a readable status. Integrity checks are read-only. They do not create probe files, enumerate installed applications, request broad package visibility, or send their results to Glacier services.

SIGNAL	WHAT GLACIER CHECKS	RESULT HANDLING
App authenticity	Installed signing-certificate SHA-256 values against the configured official allowlist.	A match passes; a missing allowlist or unreadable certificate produces unknown.
Release build	Whether a non-debug build is marked debuggable.	An unexpected debuggable release is a high-confidence risk.
Root indicators	Inspectable su, Magisk, test-key, and related filesystem indicators.	Positive results are medium-confidence heuristic evidence.
Modified environment	Selected Frida, hook-library, and process-thread indicators.	Positive results are medium-confidence heuristic evidence.
Debugger and USB debugging	Attached debugger state and Android's ADB-enabled setting.	Observed values produce high-confidence warnings.
System proxy	Android's default proxy and the runtime HTTP proxy property.	An observed proxy is shown for customer review.
Screen lock and biometrics	Secure keyguard and AndroidX biometric capability or enrollment.	The app links to the relevant Android settings when action is available.
Version currency	Android security patch age and the installed Glacier version against Play or backend metadata.	Unknown data remains unknown; it is not converted to a clean result.
Protection path and health	Live tunnel mode, packet-engine state, DNS response, and data-plane evidence.	Disconnected and degraded paths are reported separately from checks still running.

Table 4. Signals evaluated by the Security Hub and how each result is handled.

HOW TO READ THE RESULT

Local checks, with unknown kept distinct from clean

An all-clear status means the applicable checks completed without a reported finding. Root and hook checks are heuristic, and Android limits what a sandboxed app can observe. Customers should still keep Android current and use a strong screen lock.

07 APPLICATION AND LOCAL DATA SECURITY

Configuration and records have separate protections

Encrypted WireGuard configuration

Glacier stores the downloaded WireGuard profile in EncryptedSharedPreferences. Preference keys use AES-256 SIV, values use AES-256 GCM, and the MasterKey uses the Android Keystore through the AndroidX Security API. The app clears this store synchronously during account exit. [S4] [S10]

App-private records and backup

Phone-account records and call history use a Room database in the application's private storage. Other apps do not receive direct access to that database under Android's application sandbox. Glacier sets `android:allowBackup` to false, requesting exclusion from Android's automatic backup. Device-to-device transfer behavior can still vary by Android version and device maker. [S7]

The current Android source does not apply SQLCipher or another application-level encryption layer to the Room database. Android device encryption and the screen lock remain important for local records when the device is not in use.

Authenticated service requests

AWS Amplify and Amazon Cognito handle account authentication. Glacier caches the current access token in memory for API requests, attaches it as a bearer token, serializes refresh during concurrent 401 responses, and retries once with the refreshed token. Only Cognito's expired or revoked result marks a session dead. Authentication calls have explicit deadlines, and a sign-in is accepted only after Cognito reports a completed authenticated session.

TLS and profile download controls

The Glacier API client performs normal TLS validation and requires one of four Amazon root CA public-key pins for the configured API host. The separate profile-download client sends no Cognito Authorization header, constrains every redirect, and applies the same root-CA pin set to admitted hosts.

Release logging and screen capture

Release builds disable OkHttp request and response body logging. Debug logging redacts Authorization and Cookie headers. Customers can also turn off screenshots in Privacy Settings. Glacier then applies Android `FLAG_SECURE` to block ordinary screenshots, screen recording output,

and the app switcher's preview for the Glacier window. [S9]

08 SECURITY REVIEW UPDATES

Changes following the security review

The reviewed Android revision includes the following controls added or strengthened during the recent audit and release-hardening work. Each Android row below is source-verified. The Console rows match the backend evidence used in the iOS whitepaper.

AREA	IMPLEMENTED CHANGE	CUSTOMER PROTECTION
VPN profile delivery	HTTPS-only allowlist, redirect checks, CA pins, total deadline, size cap, and profile-shape validation.	Limits where sensitive profile data can be fetched and rejects malformed or oversized responses before storage.
Network secret storage	WireGuard profiles stored in encrypted preferences and erased synchronously on account exit.	Protects cached tunnel key material and prevents it from crossing account boundaries.
DNS transport	Profile-attributed DoT runs through WireGuard; marked gateway DNS requires an exact profile contract.	Removes the earlier plaintext fallback and prevents an unmarked profile from selecting the gateway path.
Tunnel health	Packet-engine, DNS, reachability, HTTPS integrity, and native WireGuard evidence drive bounded recovery.	Separates a healthy, degraded, unavailable, and disconnected path instead of trusting interface state alone.
Authentication	Bounded auth calls, completed-session validation, serialized token refresh, and Cognito-owned expiry decisions.	Prevents partial sign-in and avoids destroying local state because of a transient refresh failure.
Subscription ownership	Google Play purchases are linked to the signed-in account and account-specific entitlements are kept separate.	Reduces cross-account purchase and phone-line assignment errors on a shared device.
Account exit	Call registration, tunnel state, encrypted profiles, entitlement caches, phone records, history alerts, and account settings are cleared through one coordinator.	A failed remote sign-out does not skip the local privacy cleanup requested by the customer.
Dependency scanning	CodeQL covers Kotlin; scheduled scans inspect the resolved JVM release classpath and the shipped Go library for reachable advisories.	Extends vulnerability checks into native and transitive dependencies that ordinary source scanning does not see.
Console boundaries	Entitlement, device ownership, number ownership, caller-ID release, provider callbacks, restricted administration, and privacy-safe diagnostics remain enforced by the reviewed backend.	Keeps the same service-side authorization and privacy controls documented in the iOS edition.

Table 5. Controls added or strengthened during the recent security review.

09 DATA TRANSPARENCY

Data movement and purpose

The table combines Android implementation evidence with Glacier policy commitments. Local means the Android app uses the information on the device. A selected value can still reach a service when the customer requests an action such as a call or profile change.

DATA CATEGORY	PURPOSE	WHERE PROCESSED	PRIVACY DESIGN
Account identity	Create and authenticate an account; recover access; deliver service.	Glacier and AWS Cognito; limited local account state.	Provider-facing resources use a random account UUID where the reviewed backend supports it.
Subscription and purchase	Establish entitlement, restore purchases, reconcile billing.	Google Play, Glacier entitlement services, or Stripe for supported web purchases.	Play purchase tokens are linked to the signed-in account before entitlement is accepted.
VPN configuration	Provision a selected gateway and operate the tunnel.	Glacier profile service, Android VpnService, VPN gateway.	The profile is encrypted locally; policy states Glacier does not keep itemized VPN activity logs.
DNS profile and totals	Route encrypted DNS, apply filtering, show aggregate activity.	Android VpnService and managed DNS service.	Reviewed profile defaults drop source IP and domain fields; policy permits aggregate numeric totals.
Calling identity and metadata	Provision numbers, place and receive calls, show history, deliver voicemail.	Glacier, Twilio, telephone network, app-private database.	A Glacier number protects the personal number; routine provider identity uses the account UUID.
Contacts	Show contacts, match numbers, start a selected call.	Android Contacts provider and an in-memory app index.	The full address book is not uploaded; a selected number enters the chosen call flow.
Security Hub results	Show device and protection conditions.	On the Android device.	Integrity checks do not send their result set to Glacier services.
Push token	Notify the app about incoming calls and service events.	Firebase Cloud Messaging, Twilio, Glacier, and local state.	A device token is a delivery identifier, not call media or message content.
Diagnostic outcomes	Troubleshoot account and delivery events without network or content detail.	Restricted Glacier administrative service; 180-day expiry.	The backend schema rejects direct identifiers, content, secrets, DNS names, VPN material, URLs, and raw errors.

DATA CATEGORY	PURPOSE	WHERE PROCESSED	PRIVACY DESIGN
Support and communications	Answer requests and send opted-in service or marketing messages.	Zendesk, MailerLite, and Glacier when submitted or enabled.	Content and contact details depend on what the customer provides.

Table 6. Every data category the product touches, its purpose, and its privacy design.

10 ANDROID PERMISSIONS

Permissions are tied to features

Glacier targets Android 14 and later in the reviewed revision. Android mediates runtime access to contacts, the microphone, notifications, nearby audio devices, location-based Wi-Fi information, and VPN control. A denied permission limits the related feature.

PERMISSION OR CAPABILITY	CUSTOMER-FACING PURPOSE	BOUNDARY
VPN consent	Create the Standard or Extra protected network interface.	Android shows a system-controlled consent dialog and permits only one active VPN per user or profile.
Contacts	Display contacts, match incoming and outgoing numbers, and start a selected call.	Glacier reads the Android Contacts provider after permission and keeps an in-memory index.
Microphone	Capture audio for a Glacier voice call.	The app requests it when a call needs audio; Twilio remains in the call path.
Notifications	Show incoming calls, missed calls, voicemail, protection status, and optional reminders.	Android 13 and later requires runtime notification permission.
Location and Wi-Fi state	Read the connected SSID for trusted-network rules.	Glacier requests fine location on the trusted-network screen; this is not used as continuous location tracking.
Bluetooth and audio settings	Detect and select Bluetooth, speaker, and earpiece routes during calls.	Applies to call audio devices and routing.
Phone-call foreground service	Keep an active Glacier call alive when the app is not foregrounded.	Glacier manages its own Twilio calls and does not become the system dialer.
Boot completed	Restore the customer's selected protection mode after reboot or app update.	The stored protection intent and current network policy are checked before reconnection.
Google Play billing	Buy and manage Glacier subscriptions and line add-ons.	Google Play processes store purchases under its terms.

Table 7. Each permission the app can request, and the boundary that applies.

Customer permission control

- Review or revoke app permissions under Android Settings → Apps → Glacier → Permissions.
- Review the active VPN under Android Settings → Network and Internet → VPN. Menu names vary by device maker.
- Use manual dialing if contact access is not needed. The microphone is still required for two-way calling.

11 SERVICE PROVIDERS AND DATA SHARING

Providers receive data for defined functions

Glacier uses providers for Android distribution, purchases, authentication, push delivery, protected DNS, support, communications, payments, and calling. Glacier's Privacy Policy states that the company does not sell, license, sublicense, or share user-submitted data and that the app contains no ads or advertising trackers. Those statements are policy commitments. [S1]

PROVIDER	ROLE	TYPICAL DATA BOUNDARY
Google Play	Android distribution and subscriptions.	Google account and purchase identifiers under Google's terms.
Firebase Cloud Messaging	Incoming-call and service notifications.	Push token and delivery data; call media is not carried in the push payload.
Amazon Web Services and Cognito	Infrastructure and account authentication.	Account identifiers, authentication events and tokens, and service requests.
NextDNS	Encrypted resolution, filtering, and aggregate counts.	UUID-named profiles; reviewed defaults drop source IP and queried-domain fields.
Twilio	Calling numbers, signalling, media transport, and voicemail.	Calling data needed for the feature; routine provisioning uses UUID identities.
Stripe	Supported non-Play purchases.	Billing and transaction data under Stripe's payment role.
Zendesk	Customer support.	Messages, attachments, contact information, and support history supplied by the customer.
MailerLite	Opted-in communications.	Email address, preferences, and campaign interaction data for that relationship.

Table 8. Providers, the function each performs, and the data boundary that applies.

Private calling and minimized identity

A Glacier number reduces direct exposure of the customer's personal number to the call recipient. Twilio documents TLS for signalling and SRTP for media between its Android Voice SDK and Twilio infrastructure. Twilio and the telephone network still process ordinary calls. [S8]

Current provisioning uses one random account UUID for Twilio number ownership, access tokens, and client routing.

12 CUSTOMER CONTROL, RETENTION, AND DELETION

Controls available in the Android app

01 **Protection state.** Turn Standard or Extra Protection on or off, choose a region, set Wi-Fi and cellular activation behavior, and review live status.

02 **Permission state.** Grant, deny, or revoke contacts, microphone, notification, location, and nearby-device access through Android Settings.

03 **Screen-capture state.** Allow or block screenshots, screen recordings, and the app-switcher preview for Glacier under Privacy Settings.

04 **Account state.** Sign out or request account deletion. Local cleanup removes the active tunnel, encrypted profile, account preferences, phone records, call history, alerts, and cached entitlements.

05 **Subscription state.** Manage Google Play subscriptions through Google Play. Deleting the Glacier account does not automatically cancel a store-managed subscription.

06 **Privacy requests.** Use the contact method in the current Privacy Policy for access, correction, or service-side removal questions. [S1]

Retention follows purpose and system

Glacier's Privacy Policy describes retaining service data only as long as needed to operate, secure, support, and comply with legal obligations. Calling records, voicemail, support correspondence, purchase records, and security records may have different operational or legal lifecycles.

The Android app asks the Console to delete the signed-in account before it clears the local session. The Console accepts the request and completes the account's service cleanup asynchronously. The app then performs local cleanup. Store subscription cancellation and provider-held record deletion remain separate operations. [S1]

OUR COMMITMENT

We describe deletion as separate operations

Account deletion, local cleanup, Google Play subscription cancellation, and deletion of provider-held records are distinct operations. We do not collapse them into one promise.

13 CLEAR PROTECTION BOUNDARIES

Protection scope by feature

PROTECTION	WHAT GLACIER PROVIDES	NECESSARY BOUNDARY
Extra Protection	An encrypted WireGuard path for supported IPv4 traffic and a gateway address visible to ordinary destinations.	HTTPS and destination privacy practices still apply beyond the gateway; current Extra blocks rather than carries IPv6.
Standard Protection	Encrypted profile-attributed DNS carried through WireGuard.	Ordinary application traffic does not use the VPN and keeps its normal network path.
DNS filtering	Encrypted resolver transport, active filtering, reviewed provider-side activity minimization, and aggregate totals.	The Glacier VpnService must be active; DNS filtering does not encrypt website content.
Calling	A Glacier number, reduced personal-number exposure, UUID account identity, and protected app-to-Twilio transport.	Twilio, carriers, and the telephone network remain in the call path.
Security Hub	Readable local checks for selected integrity, configuration, version, and protection signals.	Root and hook signals are heuristic; unknown evidence is not a pass.
Local records	Android app-private storage, automatic backup disabled in the manifest, encrypted WireGuard configuration, and account-exit cleanup.	The Room call-history database does not add an application-level encryption layer, and device-transfer behavior can vary by Android version and device maker.
Screen capture	Optional FLAG_SECURE protection for Glacier windows.	Customers choose whether to enable it, and Android documents platform limits for some capture scenarios.

Table 9. What each protection provides, and the boundary that necessarily remains.

Configuration and currency

Only one VPN can be active for an Android user or work profile. Another VPN, revoked system consent, a captive portal, or a restricted network can interrupt Glacier protection. Glacier shows the selected mode and checks the live data path so interface state alone is not treated as proof of protection.

This dated source review describes implemented design and published policy. It is not an external certification of live infrastructure. The current Privacy Policy and Terms of Use govern Glacier's current commitments.

14 SECURITY GOVERNANCE

Vulnerability reporting and supported versions

Glacier maintains a private channel for good-faith vulnerability reports. Security issues should not be submitted through a public issue tracker. [S3]

Glacier develops security fixes against the current Android codebase. The response targets below are company process commitments, not a security certification.

STAGE	PUBLISHED TARGET
Acknowledgement	Within 3 business days of the initial report.
Triage and initial assessment	Within 7 business days, including rough severity and next steps.
Status updates	At least every 14 days while the report remains open.
Coordinated disclosure	A reasonable remediation window, typically 90 days, before public disclosure.
Resolution priority	Critical and high-severity issues are prioritized for the next scheduled release; lower severity is scheduled into a future release.

Table 10. Published response targets for vulnerability reports.

Report privately

Vulnerability intake: Glacier private vulnerability form. Include the affected Android and app versions, device model, reproduction steps, impact, and non-sensitive evidence when possible.

How this paper stays current

- Glacier versions the whitepaper when material data flows, providers, retention practices, or cryptographic boundaries change.
- Glacier works to keep store disclosures, website statements, in-app permission copy, and the Privacy Policy aligned with implemented behavior.
- Independent reviews, penetration tests, and certifications are identified by their scope and date when they are available.

APPENDIX A

Control and evidence matrix

CONTROL	EVIDENCE BASIS	CUSTOMER RESULT OR SCOPE
Android VpnService boundary	Android implementation and platform documentation	Uses system VPN consent and a service protected by BIND_VPN_SERVICE.
WireGuard Extra Protection	Android implementation and WireGuard documentation	Encrypts supported IPv4 traffic to the Glacier gateway and replaces the access-network address seen by ordinary destinations.
DNS-only Standard Protection	Android VpnService routing and firestack integration	Routes DNS through WireGuard while ordinary traffic bypasses the tunnel.
Profile-attributed DNS-over-TLS	Android implementation and RFC 7858	Encrypts the resolver exchange in both protection modes.
Gateway DNS marker	Android runtime selector and profile parser	Allows gateway-forwarded profile DNS only when the profile carries and satisfies the exact rollout contract.
Account-bound DNS cache	Android DNS repository and account cleanup	Pairs resolver addresses with the current account profile and clears them on sign-out.
DNS provider activity minimization	Reviewed backend default profile and Glacier policy	Drops source IP and queried-domain fields under the reviewed default and limits Glacier reporting to aggregates.
Pseudonymous DNS profile names	Reviewed backend provider-identity services	Uses an account UUID instead of email for current provider-facing profile names.
VPN profile authorization and lifetime	Reviewed backend entitlement and profile-delivery services	Checks entitlement on profile requests and limits compatibility links to 120 seconds.
Constrained profile download	Android NetworkModule, VpnProfileSource, and WireGuardRepository	Enforces allowed sources, TLS pins, redirects, deadlines, size, and structure before encrypted storage.
Encrypted WireGuard profile store	Android EncryptedSharedPreferences implementation	Encrypts tunnel configuration keys and values with a Keystore-backed master key.

CONTROL	EVIDENCE BASIS	CUSTOMER RESULT OR SCOPE
App-private Room database	Android Room implementation and platform storage documentation	Keeps phone-account and call-history records inside application-private storage without an added SQLCipher layer.
Application backup disabled	Android manifest	Requests that Android not include Glacier application data in automatic backup.
CA public-key pinning	Android OkHttp CertificatePinner configuration	Requires Amazon root CA public keys for the Glacier API and admitted profile sources.
Release HTTP logging disabled	Android build configuration and NetworkModule	Prevents request and response body logging in release builds and redacts auth headers in debug logging.
Optional screen-capture blocking	Android FLAG_SECURE implementation and platform documentation	Lets the customer block ordinary screenshots, recordings, and recents previews for Glacier windows.
Local integrity checks	Android Security Hub implementation	Reports selected authenticity, root, hook, debug, proxy, lock, biometric, version, and protection signals without uploading the result set.
On-device contact matching	Android Contacts provider integration	Keeps the contact index on the device; selected numbers enter the chosen calling flow.
Pseudonymous Twilio identity	Reviewed backend provider-identity, token, and number services	Uses an account UUID in routine Twilio identity fields.
Calling entitlement and ownership	Reviewed backend token, number, caller-ID, release, and webhook services	Requires entitlement for new calling capability, enforces number ownership, and authenticates provider callbacks.
Restricted administrative plane	Reviewed Console infrastructure and reverse-proxy configuration	Removes public SSH, gates sensitive routes to the tailnet, encrypts root volumes, and uses short-lived deployment roles.
Privacy-safe diagnostic timeline	Reviewed Console diagnostic schema and access path	Keeps bounded outcome events for 180 days while rejecting direct identifiers, content, secrets, network activity, and raw errors.

CONTROL	EVIDENCE BASIS	CUSTOMER RESULT OR SCOPE
Twilio call transport	Glacier Android integration and Twilio documentation	Uses TLS signalling and SRTP media on the app-to-Twilio leg.
Account exit cleanup	Android account coordinator and reviewed backend lifecycle	Stops local protection, clears account-scoped data, and requests service-side account cleanup.
Private vulnerability process	Glacier Security Policy	Provides a private reporting channel and published response targets.

Table 11. Every control in this paper, its evidence basis, and the customer result.

APPENDIX B

Glossary

TERM	PLAIN-LANGUAGE DEFINITION
Aggregate	A numeric summary without the underlying itemized events, such as a blocked-query total without domain names or timestamps.
Application sandbox	Android's isolation boundary that limits one app's direct access to another app's private files and database.
CA public-key pinning	A TLS control that requires the server certificate chain to contain an allowed certificate-authority public key after normal validation passes.
DNS	The Domain Name System, which translates service names into network addresses.
DNS-over-TLS	DNS carried inside a TLS connection between a client or gateway and a resolver.
Pseudonymous identifier	An identifier that omits a direct name but can still distinguish or associate an account, device, or installation.
Room	Android's database library over SQLite. Glacier uses it for local phone-account and call-history records.
SRTP	Secure Real-time Transport Protocol, used to protect real-time media on a transport leg.
Trust boundary	A point where data protection, operator control, or visibility changes.
VpnService	The Android framework that grants an approved app a virtual network interface for VPN processing.
WireGuard	A VPN protocol that uses modern cryptography to create an authenticated encrypted IP tunnel.

Table 12. Terms used in this paper.

APPENDIX C

Source basis and references

Public sources support Glacier's policy, protocol, platform, and provider-boundary statements. Implementation evidence comes from the dated Android and reviewed Console revisions in Section 1.

S1 **Glacier Privacy Policy** — theglacierapp.com/privacy. Data-use commitments, provider list, VPN and DNS logging statements, calling-data categories, and privacy-request controls.

S2 **Android VpnService** — developer.android.com. Android's system consent, virtual-interface, service-permission, and single-active-VPN model.

S3 **Glacier vulnerability reporting** — private intake form. Glacier's private intake channel for good-faith vulnerability reports.

S4 **Android Keystore system** — developer.android.com. Android's protected cryptographic key container and key-use controls.

S5 **WireGuard protocol and cryptography** — wireguard.com/protocol. WireGuard handshake, authenticated encryption, key agreement, and protocol properties.

S6 **RFC 7858: DNS over Transport Layer Security** — datatracker.ietf.org. Internet standard defining DNS over TLS.

S7 **Android data and file storage** — developer.android.com. Android application-private storage, preferences, and database boundaries.

S8 **Twilio Voice SDK network connectivity** — twilio.com/docs. Twilio documentation for TLS signalling and SRTP media on the SDK-to-Twilio transport legs.

S9 **Android secure-window guidance** — developer.android.com. Android documentation for FLAG_SECURE and its screen-capture boundary.

S10 **Android EncryptedSharedPreferences** — developer.android.com. AndroidX behavior for encrypted preference keys and values used by the reviewed WireGuard profile store.

Reviewed Android implementation areas

- AndroidManifest permissions, VpnService declaration, application backup setting, and release build configuration.
- `GlacierVpnService`, `GlacierNetstackAdapter`, `GatewayDnsGoBackendConfig`, `VpnProfileSource`, `WireGuardRepository`, and encrypted WireGuard configuration storage.
- `DnsProvisioningRepository`, account-scoped resolver caches, connection health policy, and bounded tunnel recovery.
- `DeviceIntegrityChecks`, `DeviceSecurityChecks`, `ProtectionSecurityChecks`, screenshot control, contacts, and app-private phone records.
- Cognito authentication, token refresh, Google Play purchase linking, sign-out cleanup, and Console-backed account deletion.

Reviewed backend implementation areas

- Provider identity, managed DNS, device ownership, entitlement, VPN profile delivery, and account lifecycle services.
- Twilio token, number ownership, caller-ID, release, and webhook services.
- Authentication discovery, emailed-code enforcement, API schemas, purchase verification, and generic external error handling.
- Tailnet administrative routing, HTTP security policy, public SSH removal, encrypted storage, pinned images, and GitHub OIDC deployment configuration.
- Privacy-report aggregate DNS analytics and the allowlisted 180-day customer diagnostic outcome timeline.

Document history

VERSION	DATE	SCOPE
1.0	4 September 2026	Initial Android customer edition based on revision b2652cd, including recent security-review changes and the same reviewed Console backend controls used in the iOS whitepaper.
1.1	20 October 2026	Editorial update.

OUR PUBLICATION PRACTICE

Security transparency is a living record

For current privacy terms and customer controls, consult the published Privacy Policy and the latest supported Android release. We will revise this whitepaper when providers, data use, cryptographic boundaries, or deletion behavior change materially.