

SHOTS PRIVACY POLICY

Effective date: July 11, 2026

Last updated: August 12, 2026

Shots is a Chrome extension maintained by CodCodingCode. This Privacy Policy explains how the Shots extension (“Shots,” “we,” or “us”) handles information when you use it with Instagram.

Shots is not affiliated with, endorsed by, sponsored by, or operated by Instagram or Meta.

1. Summary

Shots runs inside your browser on Instagram. Most information handled by Shots is processed and stored locally in your Chrome browser profile.

Shots also communicates with:

- Instagram and Meta, to load profiles and messages and perform actions such as following, unfollowing, approving follow requests, uploading images, and sending direct messages.
- OpenStreetMap Foundation’s Nominatim service, when you choose to search for a location.
- A developer-operated service hosted using Vercel, for limited installation and activity telemetry and, after your affirmative onboarding consent, to record which Instagram account uses Shots.

Shots does not contain advertising SDKs, does not sell personal information, and does not use information for personalized advertising, lending, creditworthiness, or data-broker services.

2. Information Shots Handles

Information you provide or select

Shots may handle:

- Your default direct-message template.

- Custom messages you compose.
- Images you attach to direct messages.
- An optional default direct-message image.
- Gender and race or ethnicity preferences.
- A location search term and the location result you select.
- Taste-anchor Instagram profiles you select.
- Follow-back and unfollow timing choices.
- Discovery-source, personalization, safety, and interface settings.
- Feedback or support information you voluntarily send to us.

Your Instagram account and session

Shots handles:

- Your Instagram account ID and username.
- Your own Instagram profile information, such as your name, username, profile image, biography, privacy status, and verification status.
- Instagram session and CSRF values needed to make authenticated requests through your existing logged-in Instagram session.
- Temporary Instagram GraphQL request tokens, including `fb_dtsg` and `lsd`, used to authorize supported messaging operations.

GraphQL request tokens are read on demand, held in extension memory, and are not intentionally written to Shots' persistent local storage or transmitted to the Shots telemetry service.

Shots does not intentionally request your Instagram email address, phone number, or password.

Instagram information about other people

Shots may load and locally process or cache information about Instagram profiles, including:

- Instagram account IDs, usernames, display names, profile images, and biographies.
- Pronouns, privacy status, verification status, and business categories.
- Follower and following counts and relationship status.
- Mutual followers.
- Followers, following lists, suggested profiles, and friends-of-friends.
- Stories, highlights, posts, tagged posts, captions, tagged users, engagement counts, music, and coauthor information.

- Location information attached to Instagram content, which may include a place name, city, or coordinates.
- Public business contact information, including a public business email address, when Instagram returns it.

This information may concern Instagram users who do not use Shots. It is obtained through Instagram using the installer's existing Instagram session.

Messages and communications

Shots may handle:

- The recipient ID and exact text of a direct message you send.
- Images you attach to a direct message.
- Sent-message history, including recipient details, thread IDs, timestamps, message text, and delivery state.
- Compact previews of recent Instagram Direct threads, which may include participant IDs, names, the latest message text or message-type label, timestamps, inbound status, and unread status.
- The contents of a conversation when you open it in the Shots dashboard.

When you open a conversation, Shots requests recent message pages from Instagram and processes the message bodies so it can display them. Shots initially requests up to 30 messages and may request older pages when you scroll upward.

Opened conversation pages are held in extension memory while the relevant Instagram page is running. They are not intentionally written as complete conversation archives to persistent Shots storage. Compact inbox previews and Shots' own sent-message history may be stored locally as described above.

Voice recordings

When you press a microphone button in a supported message composer, Shots may ask Chrome for microphone access and create an audio recording in your browser.

In the current version:

- Recording begins only after you press the microphone control and grant browser permission.
- The recording is held locally in memory for preview.
- Voice-message delivery to Instagram is not currently implemented.
- The recording is not intentionally uploaded to Shots' servers.

- The recording is discarded when you discard it, close the relevant composer, leave or reload the page, or otherwise end the recording interface.

Activity and relationship information

Shots may locally store:

- Profiles displayed or marked as seen.
- Left and right swipes.
- Follow, unfollow, request, approval, and follow-back states.
- Pending follow-back workflows.
- Messages sent through Shots.
- Timestamps and dashboard activity.
- Dwell time and interaction measurements.
- Recommendation scores, request counters, discovery-source metadata, exploration state, and decision metadata.

Sensitive preferences and inferred information

The gender and race or ethnicity preferences you select may be considered sensitive information.

Shots may infer information about Instagram profiles, including:

- A likely gender based on names, pronouns, and other profile signals.
- A likely race or ethnicity based on names and usernames.
- Whether a profile appears to represent an individual or an organization.
- Local recommendation and visual-similarity signals.

These inferences are probabilistic and may be inaccurate.

Shots stores predicted categories, probabilities, confidence values, and model-source information locally. These predictions are used only for profile filtering, ranking, discovery, and personalization.

Shots does not use these predictions for advertising, lending, employment, housing, insurance, creditworthiness, authentication, or other consequential decisions.

Photo and visual processing

When visual personalization is enabled, Shots may process profile photos and post images locally to derive numerical visual embeddings used to rank profiles.

These embeddings:

- Are processed and stored locally.
- Are not intended to identify or authenticate a person.
- Are not transmitted to the Shots telemetry service.

Shots also includes optional photo-based gender and race classification code. The required trained photo-model files are not included in the current published package, so these photo-classification paths are inactive. This Policy will be updated before a version enabling those models is released.

3. Location Search

Location selection is optional. Shots does not use the browser Geolocation API to automatically determine your physical location.

When you enter a location and press Search, Shots sends the search term to the OpenStreetMap Foundation's Nominatim service.

Nominatim may receive:

- The location query you entered.
- Your IP address.
- Browser, device, operating-system, referring-page, date, time, and ordinary request information.

Nominatim returns information such as:

- A place name and formatted label.
- A Nominatim place ID.
- Latitude and longitude.
- A bounding box.
- A place or feature type.

Shots caches these results locally to reduce repeat requests. OpenStreetMap Foundation processes requests under its own privacy policy:

https://osmfoundation.org/wiki/Privacy_Policy

Do not enter private, confidential, or personally identifying information into the location search field.

4. Developer Telemetry

Installation and activity telemetry

Shots sends limited telemetry to:

<https://shots-install.vercel.app>

When Shots is installed or updated, it may send:

- An event type such as install or update.
- A randomly generated installation ID.
- The installed Shots version.

When Chrome starts, Shots may send an active event. Active events are limited locally to approximately once every 24 hours and contain:

- The randomly generated installation ID.
- The installed Shots version.
- The active event type.

The installation ID is generated randomly and is not derived from your Instagram account. However, it is a persistent identifier and may be linked to other telemetry submitted by the same installation.

Install, update, and active telemetry may occur before onboarding is completed.

The telemetry server and its hosting providers, including Vercel, may also receive ordinary network information such as your IP address, request time, browser or client information, and server logs.

This telemetry is used to measure installations, updates, basic product activity, and product adoption.

Instagram account identity

When you finish onboarding and press “Agree & start,” Shots sends the following to the developer-operated service:

- Your Instagram account ID.
- Your Instagram username.
- Your randomly generated Shots installation ID.
- The date and time of your consent.

- The installed Shots version.

This transmission is performed only after the onboarding screen discloses the collection and you affirmatively agree.

The information is used to identify which Instagram accounts use Shots, administer the product, respond to deletion requests, investigate misuse, and understand product adoption.

Server-side telemetry and identity records are retained for 90 days, unless they must be kept longer for security, legal compliance, dispute resolution, or abuse prevention.

To request deletion of server-side telemetry associated with your Instagram account, contact nathanyan2008p@gmail.com.

Deleting local extension data does not automatically delete records already received by the telemetry server.

5. How Shots Uses Information

Shots uses information to:

- Identify the active Instagram account.
- Keep local data separated between Instagram accounts.
- Discover, filter, rank, enrich, and display Instagram profiles.
- Apply audience, location, source, and personalization settings.
- Learn locally from swipes, interactions, and taste anchors.
- Display Instagram message previews and opened conversations.
- Send messages and images you authorize.
- Follow, unfollow, or approve follow requests you authorize.
- Detect follow-backs and perform specifically authorized pending workflows.
- Display message, reply-preview, and follow-activity dashboards.
- Avoid repeating recommendations and follow attempts.
- Apply request pacing, operational safeguards, diagnostics, and security checks.
- Measure installations, updates, and basic product activity.
- Record, after affirmative consent, which Instagram account uses Shots.

6. Chrome Permissions and Site Access

Shots requests the following Chrome permissions:

storage

Used for settings, caches, histories, pending workflows, telemetry identifiers, consent records, predictions, visual embeddings, and other local extension state.

unlimitedStorage

Used because Instagram profile caches, model data, prediction caches, message images, and other locally stored records may exceed Chrome's ordinary extension-storage quota.

scripting

Used to:

- Insert Shots into Instagram tabs that were already open when the extension was installed or updated.
- Run an owner-verified, one-time function in Instagram's page context to obtain temporary GraphQL request tokens needed for supported messaging operations.

Shots does not use this permission to download or execute remote code.

offscreen

Used to run packaged machine-learning workers outside Instagram's visible page thread. This includes local name-based race inference, organization-profile classification, and supported optional photo-model processing.

Host access

Shots requests access to:

- https://www.instagram.com/*
- https://i.instagram.com/*
- https://nominatim.openstreetmap.org/*

The first two are used for Instagram pages and authenticated Instagram API requests. Nominatim access is used only for location searches initiated by the user.

Instagram profile and post images may also be displayed from Instagram or Meta content-delivery domains through ordinary browser image loading.

The developer telemetry service does not require a manifest host permission because requests originate from the extension's service worker and are permitted by the service's CORS configuration.

7. Local Storage

Shots uses:

- `chrome.storage.local`
- `chrome.storage.session`
- Local IndexedDB databases
- Temporary JavaScript memory

Shots does not intentionally store its data using `chrome.storage.sync`.

Local storage may include:

- Settings and consent records.
- Instagram account identifiers.
- Profile and enrichment caches.
- Swipe and sent-message history.
- Pending follow-back workflows.
- Relationship and activity records.
- Direct-message previews.
- Uploaded default DM images.
- Location search results.
- Recommendation and interaction records.
- Name, organization, gender, and race prediction caches.
- Visual embeddings.
- Random installation and telemetry state.

Shots does not separately encrypt its local storage. Its protection depends on Chrome, your operating system, and the security of your browser profile and device.

8. Disclosure and External Processing

Instagram and Meta

Shots sends requests directly to Instagram using your existing Instagram session.

Depending on the feature, Instagram may receive:

- Authentication, session, CSRF, and request-token information.
- Profile, media, relationship, or thread identifiers.
- Follow, unfollow, approval, like, save, and other actions you initiate.
- Direct-message recipient IDs and message text.
- Images you choose to upload and send.
- Ordinary network metadata such as your IP address.

Instagram and Meta process this information under their own terms and privacy policies.

OpenStreetMap Foundation

When you perform a location search, Shots sends the search term to OpenStreetMap Foundation's Nominatim service. OpenStreetMap Foundation processes that request under its own privacy policy.

CodCodingCode and Vercel

The developer-operated telemetry service receives the telemetry and account-identity information described in Section 4.

The service is hosted using Vercel. Vercel may process request and infrastructure information when providing hosting, security, logging, and delivery services.

Chrome and your device

Chrome supplies the extension runtime, permission controls, local storage APIs, IndexedDB, and microphone permission interface.

Although Shots does not use Chrome Sync for its data, Chrome, your operating system, enterprise-management software, backups, or browser-profile tools may handle the underlying local files according to their own settings and policies.

Other parties

Shots does not sell extension data or share it with advertising networks or data brokers.

Information may be disclosed when reasonably necessary to:

- Comply with applicable law or a valid legal request.
- Protect users, the public, or the security and integrity of Shots.
- Investigate fraud, abuse, spam, malware, or unauthorized use.
- Complete a merger, acquisition, or sale of the service, subject to applicable consent and notice requirements.

9. Retention

Profile and enrichment caches

Shots keeps bounded local profile and enrichment caches. Cache entries generally have approximately 24-hour freshness, but expired entries may be ignored rather than immediately deleted.

Sent-message history

Up to approximately 500 entries may be retained locally.

Swipe history

Up to approximately 2,000 entries per Instagram account may be retained locally.

Pending follow-back records

Pending workflows may remain active for the follow-back window you select, up to seven days. Completed or expired pending records may remain for approximately seven additional days before cleanup.

Direct-message previews

Shots stores the latest preview snapshot until it is overwritten, reset, or deleted.

Full conversation pages opened in the dashboard are held in memory rather than intentionally persisted as a complete conversation archive.

Location results

Nominatim results are treated as fresh for approximately 30 days. Stale cache entries may remain locally until local data is deleted.

Prediction caches

The current version uses bounded local caches of approximately:

- 5,000 name-gender predictions.
- 5,000 name-race predictions.
- 5,000 organization-profile predictions.
- 2,000 optional photo-race predictions.

- 2,000 optional photo-gender predictions.

Prediction caches do not currently have a general time-based expiration.

Uploaded default DM images

Default DM images are stored locally without an automatic time-based expiration. Replacing or removing a default image may not immediately remove all previously stored image bytes.

They remain until “Delete local data” is used, the extension’s stored data is otherwise cleared, or the extension is uninstalled and Chrome removes its data.

Recommendation records and visual embeddings

Recommendation and decision records are bounded by entry count or age. Some recommendation records may remain for approximately 180 days. Visual embeddings may remain until reset, local deletion, or uninstall.

Core IndexedDB records and settings

Some profile, relationship, activity, settings, taste, and account-state records do not have a general time-based expiration.

Local telemetry identifiers

The installation ID and local telemetry state remain until local extension data is deleted or the extension is uninstalled.

If Shots remains installed after local deletion, a future startup may generate a new installation ID and resume telemetry collection.

Server telemetry

Server-side telemetry and account-identity records are retained for [SERVER RETENTION PERIOD], subject to the exceptions described in Section 4.

10. Your Choices and Deletion

You may:

- Change your filters, location, message template, and personalization settings.

- Disable photo-based visual personalization.
- Skip optional location selection.
- Deny or revoke microphone access through Chrome or operating-system settings.
- Pause Shots through the extension popup.
- Reset onboarding and recommendation state.
- Delete all locally stored Shots data.
- Uninstall Shots to stop future extension activity.
- Request deletion of server-side account information by contacting [\[CONTACT EMAIL\]](#).

Reset

Shots' Reset function clears much of its operational, recommendation, onboarding, relationship, and dashboard state.

Reset is not a complete privacy deletion. It may leave:

- Settings.
- Uploaded default DM images.
- Current-user cache information.
- Prediction caches.
- Local installation telemetry identifiers.
- Request pacing and safety counters.
- Other extension records not included in the operational reset.

Reset may also cause onboarding and its consent screens to appear again.

Delete local data

The extension popup contains a "Delete local data" control. After confirmation, it clears Shots-owned:

- `chrome.storage.local` data.
- `chrome.storage.session` data.
- Relationship IndexedDB data.
- Profile and cache IndexedDB data.
- Active offscreen inference state.

This action deletes extension-local information but does not:

- Retract messages or images sent to Instagram.

- Undo follows or other Instagram actions.
- Delete information retained by Instagram or Meta.
- Delete queries or logs retained by OpenStreetMap Foundation.
- Delete telemetry already received by the developer-operated service.

If Shots remains installed, future use may create new local records and telemetry identifiers.

Remote deletion

To request deletion of server-side records associated with your Instagram username or account ID, email [\[CONTACT EMAIL\]](#).

The request may require reasonable verification that you control the Instagram account concerned.

11. Security

Shots uses HTTPS when communicating with Instagram, Nominatim, and the developer-operated telemetry service.

Shots applies account-binding and sender checks around sensitive Instagram operations. An operation may be refused when the active Instagram account does not match the account that requested it.

Temporary GraphQL request tokens are obtained through a private extension-controlled channel and kept in extension memory.

Local extension storage is not separately encrypted by Shots. No browser extension, local storage system, or transmission method can be guaranteed completely secure.

You are responsible for protecting your Chrome profile, Instagram account, device, and operating-system account.

12. Chrome Web Store Limited Use

Shots uses information obtained through Chrome extension APIs only to provide or improve its disclosed single purpose: Instagram profile discovery, filtering, personalization, follow and messaging workflows, local dashboards, and related security, reliability, and product-operation functions.

Shots' use and transfer of user data complies with the Chrome Web Store User Data Policy, including its Limited Use requirements.

Shots does not:

- Sell user data.
- Use user data for personalized advertising.
- Transfer user data to advertising networks or data brokers.
- Use user data for lending or creditworthiness decisions.
- Use demographic predictions for consequential decisions.

Human access to developer-operated server data is limited to authorized operational, support, security, deletion-request, and legal purposes consistent with this Policy and the consent provided by the user.

13. Changes to This Policy

We may update this Privacy Policy when Shots' features, service providers, permissions, models, or data practices change.

The "Last updated" date will identify the latest revision. Material changes will be disclosed before or together with the extension update that introduces them, and additional consent will be requested when required.

14. Contact

For privacy questions, support, or server-side deletion requests, contact:

CodCodingCode

Email: Nathan Yan 2008p@gmail.com

Make sure the Chrome Developer Dashboard disclosures match this policy exactly. Google states that discrepancies between an extension's behavior, dashboard declarations, and privacy policy can violate Chrome Web Store policies. [Chrome Web Store User Data FAQ](#)