November 10, 2026 · Download the PDF

Law Enforcement Guide

This guide is for law enforcement and government agencies requesting information about our members. It explains how to submit a request, how we verify it, the legal process we require, and what data we hold.

On this page

About Hey, It's You!

How to submit a request

Officer verification

Legal process required

Emergency disclosure

Preservation requests

Data we hold and retention

What we can't provide

Records format and delivery

About Hey, It's You!

Hey, It's You! is an iPhone and Android app that helps people who met in person connect again: a member shows a live code in the app, the other person scans it, and they can message and meet privately. Members use the app; the website keeps only public pages. The service is operated by BluNET Holding Company, LLC and is available in the United States, Canada and Mexico.

How to submit a request

Send requests to legal@heyitsyouagain.com. Our request portal opens soon. We don't accept requests through social media or member support.

Officer verification

We verify every request before acting on it, either by a confirmation sent to the officer's government (.gov) or other approved agency email address, or by calling the agency back on a number we look up independently. Emergency requests always include a dispatch call-back, even when the request comes from a .gov email address.

Legal process required

Requests must come with valid legal process: a subpoena, court order or search warrant. Unless the process forbids it or an emergency applies, we notify the member and release records 7 days after the notice. We may push back on requests that are overly broad or unclear. What we need depends on the records you ask for:

- **Subscriber information:** a subpoena.
- **Transaction records:** a court order.
- **Message content and ID images:** a search warrant.

Emergency disclosure

We may disclose information without legal process when a request shows an imminent danger of death or serious physical injury. Include what the emergency is, who is at risk, and why the information is needed now. We report apparent child sexual abuse material to the National Center for Missing & Exploited Children (NCMEC) through its CyberTipline, as 18 U.S.C. § 2258A requires, and we keep the evidence as the law requires.

Preservation requests

Submit a preservation request through the portal to keep a named account's records. Once the request is verified, we preserve those records for 90 days, and we can extend that once, by another 90 days. Preservation discloses nothing.

Data we hold and retention

Data	How long we keep it
Account basics (name, preferred name, email, phone, date of birth)	While the account exists. A deletion request hides the account and starts a 30-day period to cancel; then it is deleted within 15 days, except the records below.
ID verification	The check is run by our identity verification provider; we keep the result and one encrypted copy of the ID document images until a newer verified ID replaces it or the account is deleted (finished within 45 days of the request), and at most 10 years from the check, unless a legal hold or a preservation request covers the account. ID copies our team requests: deleted 30 days after the decision, unless a legal hold applies.
Selfie and face-match data	Not stored by us. Our identity verification provider deletes it once the check has a final result; when the check opens our team's photo review, it stays there until our team decides, and no longer than 24 hours after the check.
Profile photos (current and previous)	Every upload, including replaced, removed, reported or staff-removed ones, for 10 years from its upload or until the account is deleted (finished within 45 days of the request),

Data	How long we keep it
	whichever comes first, unless a legal hold or a preservation request covers the account; then deleted automatically.
Connections (who connected with whom, when)	While the account exists; deleted with the account, within 45 days of a deletion request, unless a legal or safety hold applies.
Scan and meetup locations (where a code was scanned; “I’m here!” check-ins and meetup ratings)	Scan locations stay with the connection and follow its deletion and legal-hold rules; check-in and rating locations recorded on the website stay with the meetup for 10 years, including after an account is deleted.
Meetups (time, place, meet ID, confirmations, check-ins, emergency-contact shares)	10 years, including after an account is deleted.
Messages	While the account exists; deleted with the account, within 45 days of a deletion request, unless a legal or safety hold keeps the conversation.
Blocked messages (contact details or money requests)	Kept encrypted for 7 days so repeated attempts can be counted; a message under review or kept blocked is kept as a safety record.
Payment records (store purchases)	Account ID, product, date and the store’s reference, never card details, for 10 years, including after an account is deleted.
App crash reports and website statistics	Crash and performance reports and anonymous usage counts from the app are tied only to a random installation ID and

Data	How long we keep it
	deleted after 90 days; website visit statistics are anonymous, with no IP address stored. Neither identifies a member.
Reports and staff actions	Staff access and action logs and support notes: 10 years from each event. Reports follow the reported account's deletion and legal-hold rules.
Legal and safety holds	A hold keeps the records it covers, including connected conversations, for the length our team sets, up to a year at a time, and it is renewed while police or a court ask us to keep them. Nothing about a member under a hold is deleted while it lasts. When a hold ends, the records follow the rules above again.
Security and audit logs	10 years from each event, including after an account is deleted.
Backups	Hosting and delivery-provider copies and backups follow those providers' retention processes and aren't guaranteed to disappear at the same moment as the live database.

What we can't provide

We can't provide data we don't hold: the ID-check selfie and biometric data (held by our identity verification provider only until the check has a final result, at most 24 hours when it opens a photo review), face data from our own photo checks (we keep only a match result, never a face template), messages or blocked messages after their retention period, or a member's live or

continuous location, which we never record. We can't provide content from other apps or services.

Records format and delivery

Records are delivered through a secure link emailed to the officer's confirmed address. It works for 7 days and up to 3 downloads, and the archive is a ZIP of JSON files with a manifest. A business records declaration is available on request.