Wire Privacy Whitepaper

Wire Swiss GmbH*

July 19, 2021

Contents

1 Introduction

This document provides an overview of the data and metadata that Wire collects from users and how it is used to enable certain features of the application.

*privacy@wire.com

2 Users

2.1 Profiles

Every registered user has an associated profile that contains the data that was provided during registration or that was subsequently edited:

- Username and display name
- Profile picture, including metadata about a previously uploaded public profile picture, including a unique ID, dimensions and a tag
- Accent colour
- Locale: An IETF language tag representing the user's preferred language
- Cookie Label: A label to associate with the user token that is returned as an HTTP cookie upon successful registration
- App settings: Preferences such as emoji setting, link preview setting, sound alert setting
- Wire Pro & Enterprise: Additional profile information that may be added to the profile by SCIM integration

2.2 User devices

The following data will also be collected when a new device is enrolled:

- Class: The device class: Mobile, Tablet or Desktop.
- Model: The device model, e.g. iPhone X.
- Label: A human-readable label for the user to distinguish devices of the same class and model.
- Cookie label: A cookie label links the device to authentication cookies (see Security Whitepaper).
- Timestamp: The UTC timestamp when the device was registered.
- Location: The geographic coordinates of the IP address used to register.

2.3 Connections

A registered user with a verified identity (e-mail address or phone number) can establish connections to other registered users.

Connections are established when one user sends a connection request to another and that request is accepted. A private 1:1 conversation is established between the two users in which they can exchange messages and make calls.

A user can block a connection at any time, after which further messages or calls from the blocked user will not be received. Furthermore, a user can not be

added to a conversation by someone they blocked (see section 3.1). The blocked user is not actively notified that they have been blocked.

2.4 People search

People search can be used to find other Wire users. A user can search for contacts by name or by username. Wire Pro & Enterprise users can only be found from outside their team with their exact username.

3 Conversations

Conversations are separate from each other, and a user has to be part of a conversation to receive content.

3.1 Membership

Wire distinguishes 3 types of conversations:

- 1:1 conversations which are created implicitly as a result of a connection between two users (see section 2.3). No new participants can join the conversation.
- Group conversations. Participants of the group can add other users that they are connected to (i.e. a user can not be added to a conversation by someone whom he blocked, cf. section 2.3). Every participant of a group conversation, including the creator, is free to leave the conversation at any time.
- Guest rooms, where guest are invited through a specific link for a certain group conversation. Guests don't have to create an account and can instead be a participant for 24h in the conversation. If they have an account, they can also join for longer when logged in with that account.

3.2 Group data

Wire maintains the following group data about conversations on the backend servers:

- Creator: The user who created the conversation.
- Timestamp: The UTC timestamp when the conversation was created.
- Participants list: The list of users who are participants of that conversation and their devices. This information is used by clients to display participants of the group and to perform end-to-end encryption between clients (see the Wire Security Whitepaper for further details).
- Conversation name: Every user can name or rename a group conversation.

- Role: Users can have different roles within a group: Group admin, group member (for Wire Pro & Enterprise also guest & external partner).

The above data is encrypted using transport encryption between the clients and the server.

3.3 Folders

Wire conversations can be organized into user defined folders. Wire maintains the list of folders and the list of conversations in them.

4 Wire Pro & Enterprise

Wire Pro & Enterprise use the same technology and data as personal accounts, with the addition of the team membership for team accounts. Every team has at least one member, team admin and team owner.

Team owners can specify a billing address for invoicing purposes.

4.1 Billing

Payment information (such as credit card data) is exclusively handled by billing providers [3] and is not available to Wire. Furthermore billing providers handle subscription information to determine invoice amounts. No personally identifiable user data from Wire is shared with billing providers.

4.2 Telemetry

For Wire Pro accounts, Wire client applications can collect telemetry data with the aim of improving future versions of Wire. Telemetry data helps Wire engineers to assess how Wire is used and to identify areas of improvement. Telemetry data is not tied to any other user data.

Telemetry data aggregates the various metrics of the application's usage, such as the amount of text messages sent, images posted and calls placed as well as user interface flow data and events, such as a dropped call. The exact numbers of events are rounded wherever possible.

To collect telemetry data, Wire uses the Countly framework [1] and the data is stored on a Countly server instance hosted and operated by Wire.

Users can disable telemetry data collection at any time.

5 Crash reports

Crash reports are the version-specific per-event application state snapshots generated in the event of an execution failure. Usually the crash reports are generated when the application was terminated unexpectedly by the operating system.

Wire for iOS uses AppCenter [2] for crash reports. Sending crash reports is opt-in, when enabled users can always opt-out again.

Crash reports help Wire to understand what went wrong and to release bugfixes faster.

6 Logs

Server-side logs are only kept for a maximum of 72 hours, for the sole purpose of facilitating troubleshooting, improving the service and preventing abuse.

Client-side logs are kept locally on clients and users can decide to manually share them.

References

[1] `https://stripe.com`

[2] `https://count.ly`

[3] `https://appcenter.ms`