Wire Privacy Whitepaper

Wire Swiss GmbH*

March 3, 2016

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. The profile data of a user is accessible in three forms:

- Self profile: The self profile contains all profile data and is accessible only to the user.
- Connections: Users with whom an accepted connection exists (see 2.2) have access to the profile name, accent color and profile picture, as well as a e-mail address and phone number.
- Others: Any other registered user has access to the profile name, accent color and profile picture.

2.2 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.

Connections may be established automatically if one of the users chooses to share their address book with Wire, allowing it to perform contact matching as described in 2.3.

2.3 Address Books

Address books are uploaded to backend servers if users grant client applications access to their contacts. Each address book entry is first normalized, i.e. phone numbers are ensured to be in E.164 form. Entries are then hashed (using SHA-256) and base-64 encoded before being transmitted to the server.

No other information, such as names, addresses, birthdates, notes, etc. are extracted from the address books.

Address books are checked for changes every 24h by clients and changes are uploaded again.

Uploaded address books are used to match users on Wire, i.e. to suggest new contacts and to automatically create connections between users (see section 2.2).

The matching algorithm creates connections between users who have each others e-mail address or phone number in their address book.

2.4 People search

People search can be used to find other Wire users. A user can search for contacts by profile name or by e-mail address; only complete e-mail addresses can be used as search terms.

Search results are ordered based on time and frequency of communication.

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 two types of conversations:

- 1:1 conversations which are created implicitly as a result of a connection between two users (see section 2.2). No new participants can join the conversation.
- Group conversations with up to 128 participants. 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 2.2). Every participant of a group conversation, including the creator, is free to leave the conversation at any time. The creator of a conversation has no special privileges.

3.2 Metadata

Wire maintains the following metadata 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 Wire Security Whitepaper for further details).
- Conversation name: Every user can name or rename a group conversation. Conversation names are not encrypted.

4 Usage data

Wire client applications collect usage data with the aim of improving future versions of Wire. Usage data helps Wire engineers to assess how Wire is used and to identify areas of improvement.

Users can disable usage data collection at any time.

4.1 Personally Identifiable Information

In order to shield personally identifiable information from external services, every registered user is assigned a *tracking ID*, a version 4 UUID that is distinct from the user ID. No user has access to another users' tracking ID.

The tracking ID can be used by client applications in place of the user ID when collecting usage data that is sent to external services. This protects the user's privacy, since the external service cannot match tracking IDs to Wire user IDs, and thus potentially to verified identities.

4.2 Types of usage data

Wire client applications collect several types of usage data:

- Crash reports
- Viewed screens data
- Aggregated usage statistics
- App events data

4.2.1 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.

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

4.2.2 Aggregated usage statistics

This type of 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.

This statistical data helps Wire to improve future versions.

4.3 Usage and storage

Initially the data collected is stored on the users' devices. It is synchronized periodically with Wire and third-party services and when the application is launched and terminated.

4.4 Third-party services

Some of the usage data is stored on external services. Crash reports are stored on HockeyApp [2]. All other types of usage data are stored on the Localytics [1] service.

References

[1] `http://www.localytics.com`

[2] `http://hockeyapp.net`