

# Wire Privacy Whitepaper

Wire Swiss GmbH\*

March 2, 2017

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Users</b>	<b>2</b>
2.1	Profiles . . . . .	2
2.2	Connections . . . . .	2
2.3	Address Books . . . . .	2
2.4	People search . . . . .	3
<b>3</b>	<b>Conversations</b>	<b>3</b>
3.1	Membership . . . . .	3
3.2	Metadata . . . . .	3
<b>4</b>	<b>Usage data</b>	<b>3</b>
4.1	Types of usage data . . . . .	4
4.1.1	Crash reports . . . . .	4
4.1.2	Aggregated usage statistics . . . . .	4
4.2	Usage and storage . . . . .	4
<b>5</b>	<b>Logs</b>	<b>4</b>

## 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](mailto: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, phone number and locale.
- 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 never stored on backend servers. If users grant client applications access to their address book, only email addresses and phone numbers are accessed. Each address book entry is hashed (using SHA-256) before being transmitted to the server. Those hashes are used to connect users (see section 2.2), but are only kept in volatile memory and not persisted.

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

## 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.

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. Usage data doesn't contain personally identifiable information.

Users can disable usage data collection at any time.

## 4.1 Types of usage data

Wire client applications collect several types of usage data:

- Crash reports
- Aggregated usage statistics

### 4.1.1 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.

### 4.1.2 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.

## 4.2 Usage and storage

Initially the data collected is stored on the users' devices. It is synchronized periodically with Wire and third-party services. Crash reports are stored on HockeyApp [2]. All other types of usage data are stored on the Localytics [1] service.

## 5 Logs

Logs are only kept for 72 hours, for the sole purpose of facilitating troubleshooting, improving the service and preventing abuse.

## References

- [1] <http://www.localytics.com>
- [2] <http://hockeyapp.net>