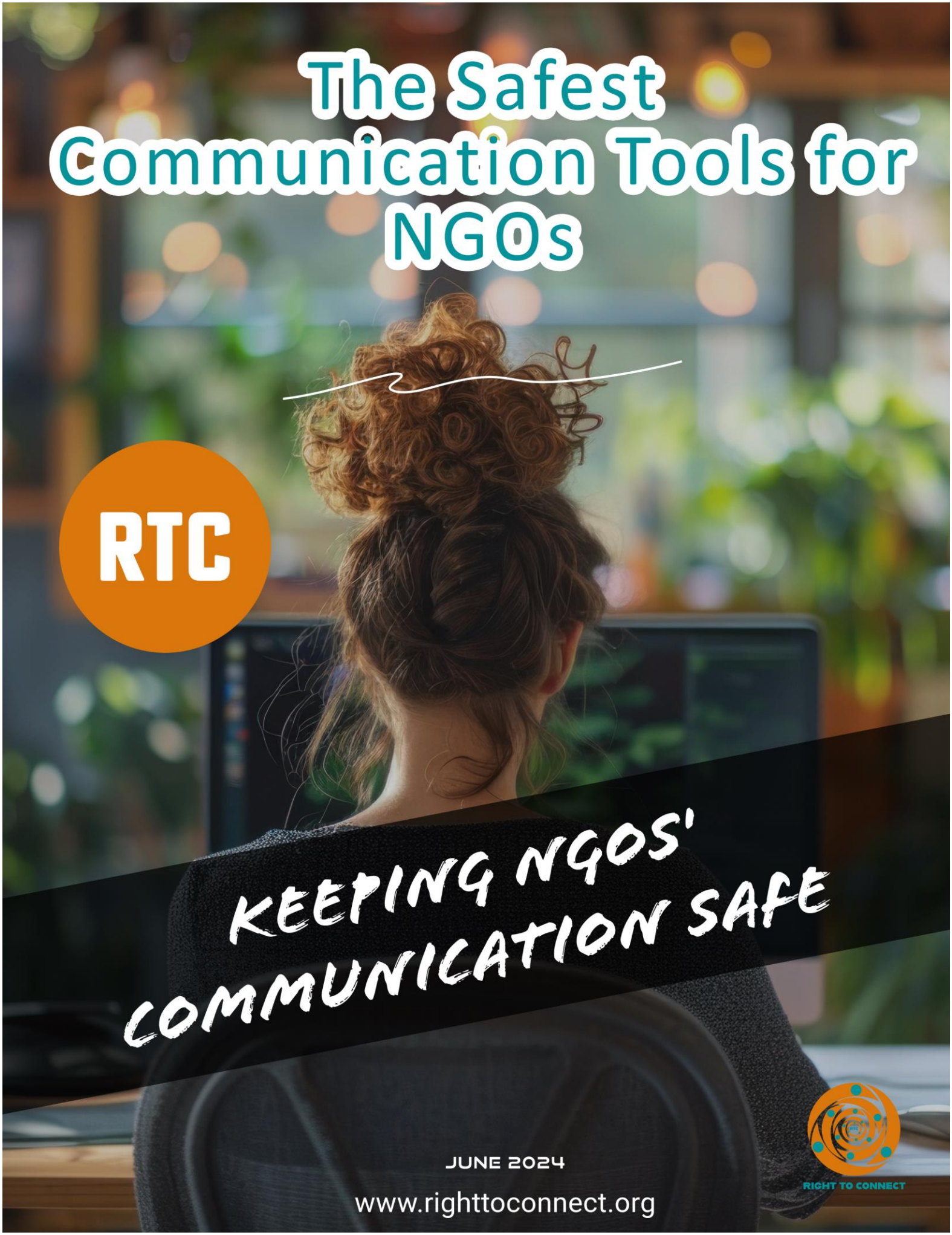
The Safest Communication Tools for NGOs



RTC

KEEPING NGOS' COMMUNICATION SAFE

JUNE 2024

www.righttoconnect.org

RIGHT TO CONNECT

SAFEST COMMUNICATION TOOLS FOR NGOS

Table of Contents

Disclaimer:

The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of our donors and RTC. While RTC retains the intellectual property rights of these guidelines, individuals and organizations are authorized to use, reproduce, and distribute any part of this material solely for non-commercial, educational, or scholarly purposes, provided that the use is accompanied by an acknowledgment of the copyright holder's name and a citation of the original source.

Our Facebook *Our LinkedIn* *Our Twitter/ X* *Our Instagram*

What are the safest communication tools for NGOs?

Apart from a few, none of these communication tools are completely secure. Select them based on your communication sensitivities.

SAFEST COMMUNICATION TOOLS FOR NGOS

Tool	Encryption sensitivity	Data Privacy	Security Features
Signal	Uses end-to-end encryption by default for all messages, calls, and media shared, utilizing its own open-source Signal Protocol.	Collects minimal user data, with a focus on maintaining user privacy. It doesn't store messages on its servers once they've been delivered.	Offers self-destructing messages, screen security (prevents screenshotting), and registration lock (PIN to protect account).

Tool	Encryption sensitivity	Data Privacy	Security Features
Wire	Utilizes end-to-end encryption for text, voice, video, and files using the Proteus protocol, built on the Signal Protocol.	Collects some user information, including user ID, phone number (if provided), and email address (if provided), for account management purposes.	Supports features like timed messages, which automatically delete after a set period, enhancing privacy. Additionally, it offers user verification to prevent man-in-the-middle attacks.

Tool	Encryption sensitivity	Data Privacy	Security Features
Threema	Provides end-to-end encryptions for all communications, including messages, calls, and files. It uses the NaCl cryptography library, ensuring that only the communicating users can read the messages.	Designed for maximum data economy, not requiring an email or phone number to sign up. It generates a random Threema ID for each user, enhancing anonymity. Contact lists and group information are stored only on user devices, not on servers.	Includes a unique feature allowing users to verify contacts with QR codes, adding an extra layer of security against potential impersonation or man-in-the-middle attacks. It also offers encrypted backups and a poll feature within chats, maintaining encryption.

Tool	Encryption sensitivity	Data Privacy	Security Features
Session	Employs end-to-end encryption based on the Signal Protocol for messages. What sets Session apart is its onion routing protocol, which obscures metadata, making it difficult to determine who is communicating with whom.	Does not collect any personally identifiable information (PII) upon registration, using only session IDs for user identification. This approach maximizes privacy by not associating accounts with phone numbers or email addresses. It's designed to leave minimal digital footprints, significantly enhancing user anonymity.	The decentralized architecture and onion routing not only provide strong data privacy but also resilience against network surveillance and censorship. Session's lack of central servers means there are no central points where user data could be requested or hacked.

Tool	Encryption sensitivity	Data Privacy	Security Features
Viber	Provides end-to-end encryption by default for messages and calls.	Collects limited data compared to others, like WhatsApp or Messenger, and focuses on user privacy, requires a phone number.	Offers self-destructing messages and requires a PIN for accessing the app on a new device.

Tool	Encryption sensitivity	Data Privacy	Security Features
WhatsApp	Implements end-to-end encryption by default for messages and calls, using the Signal Protocol.	Leading to concerns about data sharing between WhatsApp and other Meta-owned platforms, despite encryption. A phone number required.	Offers two-step verification but has faced scrutiny over Meta's data handling practices.

Tool	Encryption sensitivity	Data Privacy	Security Features
Telegram	Provides end-to-end encryption in "Secret Chats" only, not in regular messages. Regular messages use client-server/server-client encryption.	Stores data on its servers to allow for syncing across devices. Has access to metadata. Phone number required.	Offers self-destructing messages in Secret Chats and has an open API for third-party apps, which might pose additional security considerations.

Tool	Encryption sensitivity	Data Privacy	Security Features
IMO	Offers encryption for voice and video calls but lacks transparency about the type of encryption for messages.	Data collection practices are not as clear-cut, raising some concerns about user privacy. Phone number required.	Provides fewer privacy controls compared to its competitors.

Tool	Encryption sensitivity	Data Privacy	Security Features
Messenger	Offers end-to-end encryption in "Secret Conversations" only. Regular messages and calls use encryption in transit but can be accessed by Facebook.	Part of the Facebook ecosystem, sharing data across platforms for targeted advertising and other purposes.	Offers optional Secret Conversations, but by default, conversations are not end-to-end encrypted.

Tool	Encryption sensitivity	Data Privacy	Security Features
Delta Chat	Uses Autocrypt to automatically encrypt emails when communicating with other Autocrypt-enabled users.	Relies on email protocols, providing a decentralized system. Messages are stored on email servers but are encrypted.	No central servers, decentralized design, predominantly focuses on email communication security.

Tool	Encryption sensitivity	Data Privacy	Security Features
Element	Utilizes end-to-end encryption for chats and calls through the Matrix protocol.	Participants can self-host servers, increasing privacy control. However, this depends on server settings.	Supports encrypted group messaging, a variety of integrations, and customization options.

Sources

https://signal.org/
https://wire.com/
https://threema.ch/
https://getsession.org/
https://www.viber.com/
https://www.whatsapp.com/
https://telegram.org/
https://www.imo.im/
https://www.messenger.com/
https://delta.chat/
https://element.io/