SESSION

Litepaper

Send messages
Not metadata

www.getsession.org

Introduction

Throughout history, civilizations have been built on the back of private communications. For every “I have a dream,” Gandhi hunger strike, and Panama Papers, there are millions of private conversations making those moments possible. In the past, those conversations were held face-to-face, but nowadays the average conversation happens online.

In the early days the internet was a pseudonymous playground where people could create, share, and communicate. Then along came social media, which turned the internet into a digital interface for our real selves. Now, the entanglement of our ‘real’ lives and our ‘digital’ lives is seemingly impossible to avoid. While the invention of web 2.0 may have enriched our digital lives, it also ushered in a brave new world of surveillance, disinformation, and online hate.

Social media is designed to increase engagement. To achieve this, social media algorithms amplify certain kinds of participation while suppressing others. It completely misses the essence of human connection, and while it claims to give us more, or better, or new ways of connecting — it’s actually creating a world where we barely connect at all. You’re not talking to people, you’re talking to an algorithm. To repair the way we communicate online, we need to make a platform that is closer to a real conversation. It’s time to start a conversation about privacy.

Due to growing concerns over the monetisation and handling of personal data and metadata, privacy has become a key topic of concern in the tech space. People are growing tired of online surveillance, and are increasingly seeking online spaces where they don’t feel they’re being watched. Private messaging platforms provide these spaces. Messaging apps are a core part of our lives, with apps like WhatsApp, Facebook Messenger, and Telegram all boasting hundreds of millions of users. Virtually everyone with a smartphone has one (or several) of these apps installed, and sensitive personal information is shared using these messengers every single day.

But the problems with these apps are clear: collection of personal information, questionable encryption, closed source code, and centralised infrastructure...the list goes on. This tech takes control of your data — which is supposed to belong to you.

The creation of end-to-end encrypted messengers provided a big step forward for private, secure communication. But even Signal suffers from some key privacy weaknesses. However, the private messaging space still lacked an application which truly restored user control over personal data.

Session is that application. It's purpose-built for those who are privacy conscious or need to communicate sensitive information over the internet.

Problem

Some messaging apps, such as Telegram, have become enormously popular due to their excellent user experience, but lack proper privacy protections. Others, such as Tox, offer extreme privacy, but completely alien user experiences make it difficult for them to gain widespread use.

There are a few common weaknesses which are shared by many of the most popular messengers. These weaknesses give us a good overview of the state of private messaging and the issues Session needs to address.

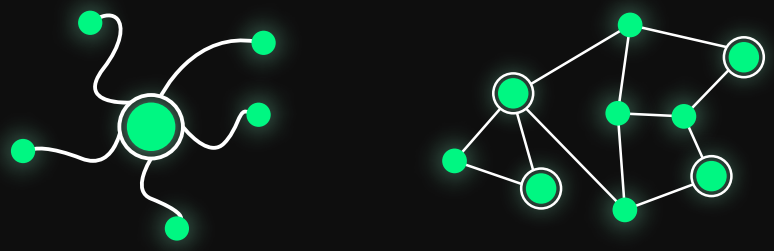
Encryption is a necessity for any messaging app. Utilising transport encryption is standard, but many either don't offer end-to-end encryption or require the user to manually enable it in their chat settings. Some messengers also use questionable encryption protocols or primitives, or simply don't disclose what kind of encryption they're using.

Messaging and social media apps usually have a sign-up process involving emails, phone numbers, or other identifying information. Users on the platform are then contactable using handles, phone numbers, or other contact information. This de-anonymises the users to the company operating the service, to the users they chat with, and (potentially) third parties such as law enforcement agencies or governments.

The issue of personal data collection for sign-up is worsened by the use of centralised infrastructure for the storage and routing of messages and other activities completed for the service. This puts service providers in control of large databases of personal information and allows for the collection and logging of sensitive metadata.

Solution

Session is a decentralised messenger that supports completely private, secure, and anonymous communications. Session provides one-on-one (direct message, or 'DM'), group chats, and voice calls.



Centralised Decentralised

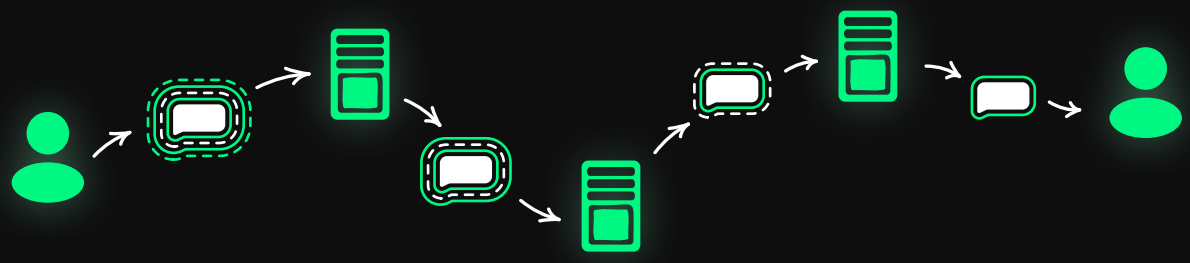
Session is a fully open source software which provides privacy, security, and identity protection suitable for almost anyone in the world, while still being usable by the average tech user.

When users sign-up to Session, their device generates a cryptographically secure Account ID. This is used as their contact information on the app. No personal information is required to create an Account ID, so you never need to link your real identity to your identity on Session. Account IDs are the public half of a public/private key pair, making them secure, recyclable, and anonymous. The private half, which is known as your Recovery Password, can be used to restore your Account ID on a new device.

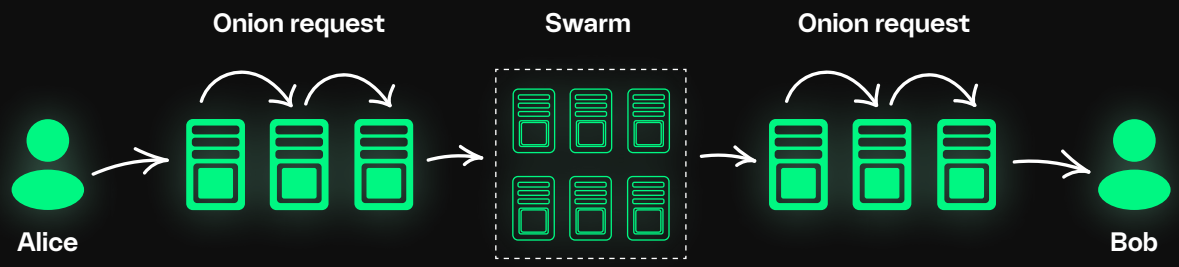
Account IDs give users a simple way to contact each other as well as being a part of Session's end-to-end encryption protocol. Because Account IDs are public keys, they can be used to encrypt a message which only the owner of that ID can decrypt. By using the keys themselves as contact information, man-in-the-middle attacks that exploit contact registries are impossible, and users have an assurance their messages will remain private and secure.

Session utilises the decentralised Session Network to store and route messages. This means that unlike P2P messaging applications you can message Session users when they are offline. This network consists of community operated nodes which are stationed all over the world. Session Nodes are organised into collections of small co-operative groups called swarms. Swarms offer additional redundancy and message delivery guarantees even if some Session Nodes become unreachable. By using this network, Session doesn't have a central point of failure, and Session's creators have no capacity to collect or store personal information about people using the app.

To protect against individual operators attempting to survey the network or collect information about users, all Session messages are onion-routed through the network. Every encrypted message is routed through three nodes in the Session Network, making it virtually impossible for the nodes to compile meaningful information about the users of the network.



When a message is sent, one node will know the sender has sent a message—but not know its destination—and a different node will know the receiver has received a message—but not know its origin.



By restricting the creation or collection of metadata or identifying information about its users, Session also gains censorship-resistant qualities. Because individual users in one-on-one and encrypted group chats cannot be identified, they cannot be personally targeted by censorship from third-parties. Session also contains open group chats intended for large communities. These open groups are hosted on federated servers operated by the communities themselves, and moderation policies are determined by each individual community.

Because of the design of the Session protocol, users can have extreme confidence that whenever they send a message that only the person they send it to will be able to know: the message contents; who they messaged; who messaged; when they sent the message.