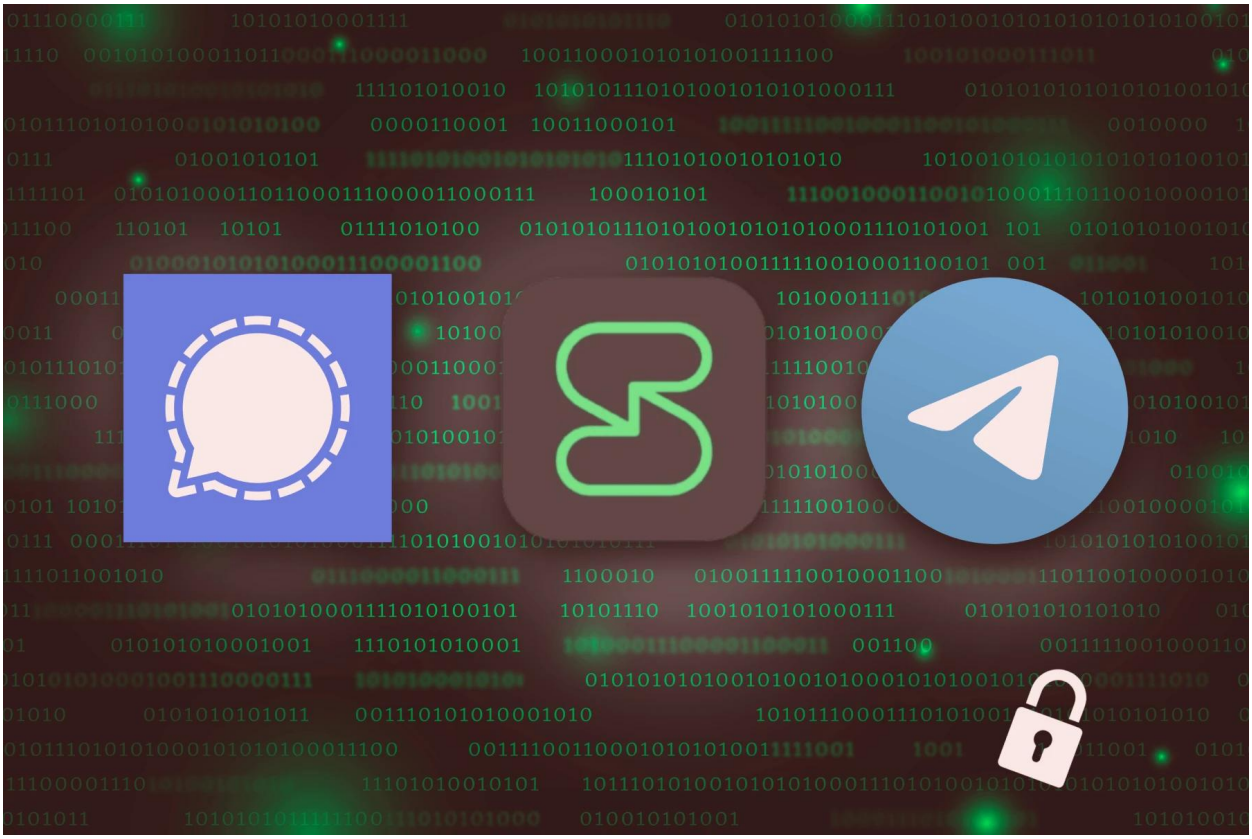
Is the Session App Truly Secure? Analyzing Its Safety Features and Privacy Concerns

حمزة حسن | August 26, 2025



This is an AI-generated English translation. The original text is in Arabic.

In oppressive political environments, such as those in the Middle East, the greatest challenge faced by an activist, journalist, or even a peaceful collaborator may be the phone they carry in their pocket. A single unprotected message could become a thread that leads security agencies to an entire network of friends and colleagues or even to the individual themselves, potentially threatening their life or work in the presence of restrictive regimes as is the case today.

Therefore, digital security at this time is a fundamental necessity and not a luxury. But the question every activist faces daily is: How do I send a sensitive message to someone, just once, and then disappear without leaving a trace?

In this article, we attempt to provide a practical framework, but we do not promise a magic solution, as we will stop at the most popular applications currently used for communication, such as Telegram and Signal, and then focus on Session as an unfamiliar tool that may offer activists a new and different option, especially in the case we are discussing here, which is one-time messages.

Surveillance is No Longer a Technical Luxury

In most of today's restrictive regimes, digital surveillance is no longer an option; it has become a policy practiced daily. The security agencies of these countries no longer need to read the texts of your messages to know a lot about you; it is sufficient for them to collect what is called metadata.

What is Metadata?

Metadata does not mean the content of the message itself, but rather the information surrounding it, and in our case, it is: who you communicated with, at what time this communication took place, from where, and how many times this communication was repeated. Ironically, this data can sometimes be more dangerous than the text of the message itself, as it reveals the "network of relationships" rather than just a single sentence.

To clarify the issue, letâs take an example: Imagine a journalist who communicated with an international human rights organization via an encrypted application. Although the authorities could not read the messages themselves, they noticed that his phone communicated multiple times with a specific international number during the night hours. This information alone is enough to raise suspicion and link this journalist to a leak or "undesirable" collaboration.

The danger is that all of this no longer requires a soldier to eavesdrop on calls or track incoming and outgoing messages; today, automated analysis programs can digest millions of records daily and process them at the click of a button, mapping out a social network that identifies who is "central," who

communicates with whom, who suddenly appears on the line, and who disappears.

For this reason, it is no longer sufficient for an activist to say, "I use an encrypted application." Even the strongest applications may leave a trace of metadata if used repeatedly or from the same device and identity to pinpoint your location, identity, and personality. What the activist really needs is a means that allows them to send a single message and then immediately erase their digital identity to minimize the impact and prevent any other party from mapping a network around them.

Why Common Tools Are Not Enough?

Many activists still rely on popular and widely used applications for communication due to their ease of use, but when we talk about sensitive one-time messages, some limitations emerge that make these programs unsuitable:

Â Â Â Â â¢ Telegram: End-to-end encryption is not activated by default except in "Secret Chats," and most users do not use it at all; in fact, many are unaware of its existence. This means that most conversations remain stored on central servers that can be accessed legally or through pressure. Moreover, Telegram requires a phone number for registration, which always ties your identity to a SIM card.

Â Â Â Â â¢ Signal: Considered the most powerful and reliable in open-source encryption, and is globally recommended for long-term communication. However, its main problem is that it only works with a phone number.

Â Â Â Â Â Â

Even if the activist tries to circumvent the number issue by purchasing a SIM card not registered in their name, activating it on any phone may reveal to the service provider (the telecommunications company) the device number (IMEI), thus linking the card to the device through which the account was activated. Additionally, the activation process also records the approximate geographical location via network towers, providing authorities with a "spatial and temporal

fingerprint" of the activation time.

To illustrate this, letâs take a real-life example:

Imagine a human rights activist wanting to send a sensitive file once via Signal. The activist buys a new SIM card, thinking it will remain anonymous, but in order to receive the activation code, they put it in their personal phone for just a minute. At that moment, the telecommunications company records this information:

Â Â Â Â 1. The SIM card number.

Â Â Â Â 2. The device number (IMEI).

Â Â Â Â 3. The geographical location of the towers that the phone connected to.

With this data, authorities can quickly narrow down the range: "The number was activated in a specific neighborhood at 9 PM, on a Samsung device with this IMEI," thus even if the number is not registered in their name, this temporal-spatial link may be enough to indicate who they are.

For this reason, despite the strength of Signal and Telegram in encryption, their reliance on phone numbers makes their use for "one-time" messages fraught with technical risks, leaving a trace that could be used against the activist, and it also comes at a high costâthe price of the lines each time they need to send a message just once.

All these limitations have driven some activists to search for alternatives that do not rely on a phone number, and in this case, the Session application emerges as a different option.

Session: Whatâs Different Here?

Unlike Signal and Telegram, which require a phone number and thus expose your identity from the moment of activation via SMS, IMEI, and geographical location, the Session application is designed to address this problem from the outset as it:

Â Â Â Â â¢ Does not require a phone number, meaning your account is not

linked to a SIM card or your personal device.

Â Â Â Â â¢ Creates a random Session ID for you, with the option to dispose of it immediately after the task is completed.

Â Â Â Â â¢ Relies on a distributed network of "nodes" (similar to Tor) which reduces the possibility of tracing the source.

Â Â Â Â â¢ Once the Session ID is deleted, the connection between you and the previous messages is severed.

However, despite these advantages, there are always important limitations and drawbacks, including:

Â Â Â Â â¢ Slow performance: This occurs because messages pass through several nodes, making communication slower, and it delays urgent messages for some time.

Â Â Â Â â¢ Storage of undelivered messages: They remain in the network for 14 days, which represents a potential window for attack if the device or intermediary nodes are targeted.

Â Â Â Â â¢ Does not protect against device hacking: If your phone is hacked, all your attempts at protection will fail regardless of the strength of the encryption because the hacker sees what you do on your phone and records all your movements on it.

Â Â Â Â â¢ Human errors: Such as reusing the same Session ID for more than one purpose, or for more than one time, keeping the application installed on your phone for a long timeâany of these issues may leave a trace on your device that can be linked back to you.

Â Â Â Â â¢ Reliance on a volunteer network: Because the application relies on a network managed by volunteers instead of a single central server, messages may sometimes be delayed or performance may fluctuate, and some network points may be weaker against targeting.

Letâs take a real example of the risks that can arise from the above:

Suppose there is an activist who wants to send the location of a sensitive meeting to one person. They create a new Session ID and send the message. However, instead of deleting the session ID or the application immediately after the message is received by the other party, they keep the application on their phone and use the same identity later with a different person. Here, there is now one technical thread linking two separate conversations, so if their phone or device is confiscated, authorities can then link the two messages together and build a network of relationships even though the encryption of the application has not been breached, but the flaw came from the user.

From the above, we conclude that:

Session offers a real solution to the problem of the phone number and IMEI through which the device and location are identified via the SIM card, which are the issues that make Telegram and Signal unsuitable for "one-time" messages.

However, it is not an absolute impenetrable fortress: slowness, caching, and human errors are all vulnerabilities that could turn it from a protective tool into an additional risk if used incorrectly.

While Session overcomes the SIM/IMEI problem that other applications suffer from, it does not completely prevent the observation that a device has used the Session application or when it was used, and this information may appear to your Internet Service Provider (ISP) or through comprehensive surveillance systems. Although the content remains encrypted, just knowing the time of use may narrow the search field if combined with other data.

Your Personal Security is More Important than Anything

For an activist living in a country that prohibits and criminalizes communication with human rights organizations or independent media, the details we mentioned are not just technical considerations; they may be a matter of great danger for them, as a single small mistake or slight digital trace may be enough to expose them to legal accountability or personal risks.

How can activists use Session on phones?

Since the phone is the primary tool for activists and the easiest, the way to use Session on it may determine the difference between a secure message and a message that turns into a thread revealing an entire network or endangering their life, so attention must be paid to those basic steps:

1. Secure Installation

Â Â Â Â Â Â - Always download the application from trusted device stores like Google Play or the App Store.

Â Â Â Â Â Â - If the store is blocked or monitored, you can use the official site (getsession.org) with a reliable VPN.

Â Â Â Â Â Â - Always check the link to avoid any fake copies that may contain spyware or tracking software.

2. Creating the Identity

Â Â Â Â â¢ When you open the application for the first time, a unique Session ID is automatically generated; this number is what you use to receive messages from other parties.

Â Â Â Â â¢ If your message is one-time, send it and wait for the "delivered" signal to appear.

Â Â Â Â â¢ Remember that any undelivered message remains in the network for up to 14 days, which represents a risk window if the device or intermediary nodes are targeted.

Â Â Â Â â¢ Once the message arrives, delete the old identity immediately. If your task is completed, it is preferable to delete the application itself to minimize any trace.

3. Privacy Settings

Â Â Â Â â¢ Disable notifications, as they pass through Google or Apple services and may leak your private data to identify you.

Â Â Â Â â¢ Disable phone or cloud backups.

Â Â Â Â â¢ Enable application lock with a password or fingerprint.

Â Â Â Â â¢ Disable camera, microphone, and location permissions from the phone settings.

Â Â Â Â â¢ Use a VPN during use, not just at installation.

4. During Use

Â Â Â Â â¢ Never send your photos or personal data, nor send any file taken with your phone unless you ensure the removal of the EXIF or metadata of the file.

Â Â Â Â â¢ It is preferable not to use the Session application on the same phone that contains your exposed accounts (WhatsApp, Gmailâ¦).

Â Â Â Â â¢ Consider the Session application as a tool for a specific task, and do not use it as a permanent chat program.

5. After Use

Â Â Â Â â¢ Once the message reaches the other party, delete the Session ID immediately.

Â Â Â Â â¢ If you no longer need the application, it is better to delete it entirely.

Â Â Â Â Â Â

Fatal Mistakes

In most cases, the tool does not betray you, but how you use it may do so, so avoid:

Â Â Â Â â¢ Reusing the same Session ID for two different purposes.

Â Â Â Â â¢ Leaving copies of messages or screenshots.

Â Â Â Â â¢ Using public Wi-Fi networks without a VPN.

Â Â Â Â â¢ Relying on a previously hacked device or a device you suspect is hacked.

Â Â Â Â â¢ Assuming that Session protects you regardless of your behavior.

Â Â Â Â â¢ In extremely risky situations, it may be dangerous to share the same device among multiple activists.

An Additional Layer of Protection

Sometimes it is not enough for the message to be encrypted or anonymous; it must disappear completely after being read. Here come services like Privnote or BurnerNote, which work simply: you write the message, get a special link, send it to the other party, and once they open it, the message disappears permanently.

This idea may seem ideal, but if used directly without precautions, it can turn into a danger:

Â Â Â Â â¢ As soon as you enter the site via a regular browser, the service provider logs your visit, knowing that you used this tool even if they do not access the content of the message.

Â Â Â Â â¢ Just the record of the time and place you entered is enough in some repressive environments to link you to a sensitive event or meeting.

Â Â Â Â â¢ Some fake sites imitate Privnote to deceive activists and steal their messages.

Â Â Â Â â¢ Even self-destructing messages do not prevent the other party from taking a screenshot or rewriting what they received.

Â Â Â Â â¢ Additionally, be aware that some devices may retain indirect traces, such as the clipboard history.

For this reason, integrating those services with Session may be a more than good way to ensure protection through multiple layers.

The Best Solution: Integration with Session

To minimize the trace you leave behind when sending messages, do not open

those sites that encrypt messages from your regular browser; instead, use them through a secure browser like Tor, so that the connection passes through an anonymous and encrypted channel.

After that, write your message and use the link, send it via Session to the other party, and as soon as you confirm the message has been received, delete the session ID and do not forget to also clean your clipboard history on your phone.

In this way, the service provider will not see that you accessed these sites because they are hidden within the Session application itself or the protected browser, and the message disappears immediately after being read; all these factors complicate leaving a digital trace and thus provide you with more protection.

However, it should be noted that:

Self-destructing messages are useful, but their danger lies in how they are used. If used directly, they may become a point of weakness. However, if used through a secure browser and then within Session, they provide activists with a practical tool to send a one-time message that disappears after being read, while minimizing the digital trace to the lowest possible extent.

What Session Does Not Protect You From?

You may be tempted to feel "protected" simply because you are using an encrypted application like Session. But in reality, Session is designed to solve a specific problem: eliminating the need for a phone number and the associated traces (SIM, IMEI, geographical location). The rest of the risks are present and may be more lethal, including, as mentioned earlier, direct hacking of the device, allowing the hacker to read and see