SIGNAL

a handbook for activists

How to protect your messages on Signal

The curious case of
the disappearing messages...

You might have heard about cases of Signal messages being recovered, even after they have 'disappeared' off the app. This has affected activists on trial in both the UK and US.

This zine will take you through steps to understand how this could happen, and things you can do to better protect your messages.

Today

Can Signal hand over my data to law enforcement?

21 May, 13:32

Many have been asking this question, following the incidents affecting activists.

13:34

In theory, Signal can be legally forced to hand over information to government or law enforcement agencies.

e.g. through a ***subpoena*** (a legal requirement to appear in court as a witness, or to hand over documents or evidence to the court)

13:38

BUT, Signal holds less data on you on its servers than some other communications services (e.g. WhatsApp). This means that even when forced to, it has less to hand over.

13:38

"Signal doesn't have access to your messages; your calls; your chat list; your files and attachments; your stories; your groups; your contacts; your stickers; your profile name or avatar; your reactions; or even the animated GIFs you search for"

13:39

Source:https://signal.org/bigbrother/santa-clara-county/

How does Signal work?

25 May, 16:34

Signal uses ***end-to-end encryption***, which means that messages are scrambled in transit (as they travel from one device to the other), until they arrive on your device. No one but the sender and recipient can read the messages.

Signal does not store your messages on its own servers. Instead, your messages are ***stored locally*** on your own device.

This has separate security implications, which we'll explore later!

Can we verify these claims?

We can never be 100% certain! But here's the info we do have:

Signal runs on an open source code, that is published online. This means independent members of the public can inspect its code to verify Signal's claims about its software. There is an active community of independent researchers and security audit firms that are doing just this.

No (publicly available) evidence from subpoenas of Signal has shown the content of messages being handed over, even when requested. This would suggest Signal actually does not possess that data, as it would be legally obliged to hand it over if it did.

Signal publishes government requests for its data online at https://signal.org/bigbrother/

(but there could be NDO/NDAs, so this list is likely not complete)

NDO (Non-Disclosure Order):
A court order prohibiting the disclosure of certain information or documents

NDA (Non-Disclosure Agreement):
A contract prohibiting the disclosure of certain information or documents to unauthorized third parties]

Example disclosure from Signal's Big Brother website page:

Signal was subpoenaed by U.S. District Court for D.C. in July 2025 for the account creation date/time and last connection date/time of 37 phone numbers. Signal says that it was able to disclose information for only 6 of these accounts.

In conclusion: Signal can hand over some limited information, like the date your account was created, or the last time you accessed it. But if you have been presented with messages that have disappeared off your app, this is likely to be using other techniques...***READ ON***

NOTIFICATION DATA

Forensic extraction software tools (see pg.16 for more details) can retrieve some of your 'disappeared' messages by going into the database of notifications on your phone.

HERE'S HOW IT WORKS:

1. The content of notification previews is often stored on a device's internal memory, which can remain after messages or even the app are deleted.

2. Forensic software can be used to access this storage system on the device and read messages that had disappeared from the app, but have been stored in your notifications database.

3. Note that as you only get notifications on incoming messages, ***this type of extraction only recovers the messages you receive, and not the messages you send.***

Notification data used in activist trials, March 2026

This evidence was used to prosecute antifascist activists in the U.S. who staged an action at the ICE Prairieland Detention Facility in July 2025.

"Messages were recovered from Sharp's phone through Apple's internal notification storage – Signal had been removed, but incoming notifications were preserved in internal memory. ***Only incoming messages were captured (no outgoing)***"*

This type of message extraction has also been used on climate and Palestine solidarity activists in the U.K. in the past few years.

Apple claims that it has fixed this issue for iPhone 11 and later, so that there is 'improved data redaction'. Note that we don't know what 'improved' means, so it's better to remain cautious about notification previews!

* https://prairielanddefendants.com/court-notes/march-10-federal-trial-day-12

ACTION POINT: KEEPING YOUR NOTIFICATION DATA SAFE

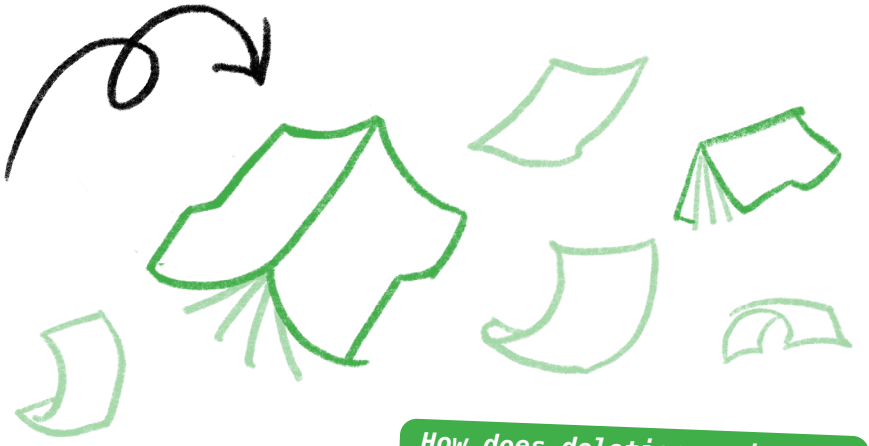
1. On the Signal app, tap your ***Profile > Notifications > Show***
2. ***Select: 'No name or message'***

You're done! This will prevent any previews or details of the sender showing in your notification previews, preventing it from being stored in any local storage on your phone!

LOCAL STORAGE

Remember reading on pg.3 that Signal stores your messages locally on your device, rather than on its servers?

If someone has your physical device and uses forensic extraction software on it, they could retrieve deleted or disappeared messages from your local phone storage that have not been fully overwritten yet on the device. To understand how this works, let's talk about how 'deleted' data works on a device.



How does deletion work on a device?

23 May, 14:36

When something is 'deleted' from your phone, it doesn't immediately disappear.

It is marked by your device as 'data that's ok to overwrite'.

As new data comes in (photos, messages, apps), it will overwrite the deleted data. Only then is it truly 'gone' from your device.

The likelihood of being able to recover deleted data from a device all depends on the capabilities of the forensic extraction software, plus the level of encryption (i.e. protection) you have as a defence against it.

SECURING YOUR PHONE AGAINST EXTRACTION

WHAT YOU CAN DO:

USE MOLLY.

It uses Signal servers but it encrypts the local database of your messages with a passkey. It is also better at overwriting/shredding of the data that's been deleted

TURN YOUR PHONE OFF (IF YOU CAN)

Before First Unlock offers an extra layer of protection if someone is trying to get into your phone.

Install Graphene OS* it automatically restarts your phone at regular intervals

*Graphene OS: a privacy & security-focused alternative operating system to Android that can be downloaded on Pixel phones (Pixel 6 & above). It installs an Android operating system without pre-installed Google Apps, and provides enhanced security features. You can find out more about these features at https://grapheneos.org/features

GOOD PASSWORD PRINCIPLES

Your lock screen is the front door to your phone: your first defence against extraction techniques. Think about the following principles for good password defence:

1. ***Long password containing letters and numbers***
2. Practice quickly activating 'Lockdown mode' to temporarily turn off biometrics (or don't use biometrics at all!)
3. Look for settings on your phone such as erase all data after 10 failed attempts

ENCRYPTION!!

Disk encryption means that all the content on your device becomes unreadable **UNLESS** the decryption key (password) is provided. Examples of encryption include:

Phone: Molly with passphrase encryption, meaning that until you enter the key the messages on your Molly app will remain encrypted

Laptops: e.g. Bitlocker for Microsoft / LUKS2 for Linux

Note that on Windows the encryption key is often stored online in your Microsoft account, which could be accessed e.g. by law enforcement or hacking

USE APPS THAT OVERWRITE YOUR DELETED DATA

There are a range of free + paid options available. e.g. Extirpater

Note that frequently overwriting may degrade the lifespan of your phone.

Think: Encryption Before Deletion

THINK ABOUT YOUR PHONE MODEL

Older phone models (especially Samsung phones) have vulnerabilities that might allow extraction software to get past your lockscreen more easily - consider this if you are selecting or using secondary phones for actions

For more details on passwords & encryption, take a look at the Digital Self Defence Zine

KNOW YOUR RIGHTS

Scan here to access the Green and Black Cross guide:
"I've been arrested: what next?"

Activists' and organisers' devices are increasingly being targeted by law enforcement. Here's some useful things to know if you get arrested or raided:

YOU DO NOT NEED TO GIVE THE POLICE YOUR PASSWORD

The police may threaten to serve you with a ***Section 49 RIPA*** notice (Regulation on the Investigatory Powers Act), which would legally obligate you to hand over your password.

This can sound scary! But until they officially serve you that notice, ***you do not have any obligation to hand over your password.***

Note: Section 49 RIPA will not be served on the spot. It requires several steps of assessment and authorisation through the policing hierarchy, including approval from the National Technical Advice Centre and a judge (normally Circuit Judge). The police would need to prove that the use of this power is proportionate to the alleged offence.

FORENSIC EXTRACTION TOOLS

Be aware: The police are increasingly using digital forensics tools to get into activists' devices. 'Digital forensics/extraction tools' basically means a type of technology that can get into a device, bypassing passwords and even encryption. That is why it is so important to secure your phone and laptops!

In the UK, there are two major suppliers of digital forensics tools to police forces: ***Cellebrite*** and ***Grayshift***.

CELLEBRITE: An Israeli company that sells digital intelligence and forensics services all over the world. It has many different forensic software offerings, but its main tool is the UFED (Universal Forensics Extraction Device)– which does what it says on the tin.

Cellebrite supplies technology to the Israeli government and military, and has been used extensively during the genocide in Gaza to harvest data from the phones of Palestinians. Cellebrite also provides services to ICE and prison agencies in the U.S., the military government in Myanmar, as well as many other regimes linked to human rights abuses.

GRAYSHIFT: Grayshift is a US company that merged with Canadian company Magnet Forensics in 2023. Grayshift developed the GrayKey tool, which works a lot like UFED to bypass mobile devices' security measures to extract data.

Further support: Check out the Digital Security Helpline run by Access Now, which provides support and advice for activists who need to secure their digital devices against increasingly invasive technologies and surveillance tactics.

MAKING YOUR OWN SECURITY MANIFESTO

Mainstream framings of security often rely on practices of policing and surveillance; whether that's top-down from institutions in power, or encouraging us to police and spy on each other. We can do better. We can build a culture that is based on collective safety rather than security logic, where we care for each other instead of policing each other.

PRINCIPLES FOR COLLECTIVE SAFETY

1 YOU CAN'T DO THIS ALONE

Safety in our organising isn't something we can achieve by downloading an app, or changing one behaviour. If we want to extract ourselves from this system, we have to do it together, one step at a time.

ACTION POINT: Do it with friends. Start a club, host a party! Choose a few things you're going to do (e.g. work down a digital hygiene checklist, start moving your data off Google) and keep each other accountable. Consider how you could make these spaces intercultural and intergenerational.

ACTIVITY

Gather with your friends, comrades, and communities you organise with. Think about practices or skills that would make you feel safer in your organising. Come up with 3 principles for collective safety, and 3 action points for getting there. Below are a few suggestions to get you started!

2 SOLIDARITY, NOT SUSPICION

Security for movement groups can be an emotional issue, because the stakes of staying safe feel so high. But if we tear each other apart in a scramble for security, we do our opponents' job for them.

ACTION POINT: Come up with a regular security hygiene check-in in your group, so that auditing security becomes a collective activity rather than something to police in people.

3 TECH IS JUST A TOOL

Technology can feel at once like the all-seeing enemy and also the silver bullet saviour. Don't give it that power. Keep informed about best practice with tech you use, but also create tech-free spaces and meetings, a little at a time. Experiment with how we can make tech work for us, not the other way around.

ACTION POINT: Practise building tech-free moments into your life: tech-free meetings, navigating without GPS.

4 ... FILL IN THE REST

This handbook was produced in June 2026, as part of the Bertha Challenge Fellowship. It is the first in a series of resources investigating how technology is being used against activists in the UK and beyond, and supporting security knowledge for movement groups and organisers.

Written by: Yuna Chang

Designed by: Bella Harter