Signal Problems

Anonymous

1 July 2026

Contents

The following are lesser-known problems with Signal that anarchists and other targets of state repression should know about. These issues are known to the Signal developers.

Potentially sensitive information is permanently saved in account databases.

Despite being hidden, the following information is permanently saved.

- All visible phone numbers: Most Signal users still have the phone numbers of all other chat members from before March 2024, when they could first change their phone number visibility to "no one."
- Group metadata: Leaving and deleting a Signal group mainly deletes the messages. The group members, the group name, the group description, the joined timestamp, the last message timestamp, the group ID, the group keys, member labels, the admins, removed members, the group link password, the draft message, the message count, the sent message count, the disappearing message time, and more are permanently saved.

Example


```
"id": "REDACTED",
"groupId": "REDACTED",
"type": "group",
"version": 2,
"expireTimerVersion": 1,
"unreadCount": 0,
"verified": 0,
"messageCount": 3,
"sentMessageCount": 2,
"name": "REDACTED",
"revision": 8,
"publicParams": "REDACTED",
"secretParams": "REDACTED",
"accessControl": {
  "members": 2,
  "attributes": 2,
  "addFromInviteLink": 4,
  "memberLabel": 2
},
"membersV2": [
  {
      "role": 2,
      "joinedAtVersion": 0,
      "aci": "REDACTED",
      "labelString": "REDACTED"
```

```
  },
  {
      "role": 1,
      "joinedAtVersion": 1,
      "aci": "REDACTED",
      "labelString": "REDACTED"
  }
],
"pendingMembersV2": [],
"active_at": null,
"avatars": [
  {REDACTED}
],
"groupVersion": 2,
"groupVerifiedNameHash": "REDACTED",
"masterKey": "REDACTED",
"profileSharing": true,
"timestamp": null,
"needsStorageServiceSync": false,
"sealedSender": 0,
"color": "A110",
"senderKeyInfo": {
  "createdAtDate": REDACTED,
  "distributionId": "REDACTED",
  "memberDevices": []
},
"lastMessage": "",
"lastMessageReceivedAt": REDACTED,
"lastMessageReceivedAtMs": REDACTED,
"lastMessageDeletedForEveryone": false,
"expireTimer": 86400,
"left": true,
"pendingAdminApprovalV2": [],
"bannedMembersV2": [
  {
      "serviceId": "REDACTED",
      "timestamp": REDACTED
  }
],
"markedUnread": false,
"unreadMentionsCount": 0,
"draft": "REDACTED",
"draftBodyRanges": [],
"draftChanged": true,
"draftIsViewOnce": false,
```

```
"storageVersion": 27,
"storageID": "REDACTED",
"description": "REDACTED",
"announcementsOnly": false,
"terminated": false,
"draftTimestamp": null,
"draftAttachments": [],
"messagesDeleted": true
```


- Contact metadata: Deleting a chat keeps the contact's name, their ACI (account identifier), their phone number, their about section, their nickname, the last message timestamp, the contact note, the draft message, the message count, the sent message count, the disappearing message time, profile keys, the profile key credential expiration timestamp, and more. Removing a contact only hides it.

Example


```
"id": "REDACTED",
"serviceId": "REDACTED",
"type": "private",
"version": 2,
"expireTimerVersion": 1,
"unreadCount": 0,
"verified": 0,
"messageCount": 4,
"sentMessageCount": 2,
"sealedSender": 1,
"color": "A110",
"profileKeyCredential": "REDACTED",
"profileKeyCredentialExpiration": REDACTED,
"accessKey": "REDACTED",
"profileKey": "REDACTED",
"profileName": "REDACTED",
"note": "",
"messageRequestResponseType": 2,
"profileSharing": false,
"storageUnknownFields": "",
"hideStory": false,
"isArchived": false,
"markedUnread": false,
"storageID": "REDACTED",
"storageVersion": 33,
"needsStorageServiceSync": true,
"muteExpiresAt": 0,
"colorFromPrimary": 2,
```

```
"about": "REDACTED",
"aboutEmoji": "",
"sharingPhoneNumber": false,
"capabilities": {
"profiles_v2": false,
"attachmentBackfill": true,
"spqr": true,
"usernameChangeSyncMessage": false
},
"lastProfile": {
"profileKey": "REDACTED",
"profileKeyVersion": "REDACTED"
},
"unreadMentionsCount": 0,
"lastMessage": "",
"lastMessageReceivedAt": REDACTED,
"lastMessageReceivedAtMs": REDACTED,
"timestamp": null,
"lastMessageDeletedForEveryone": false,
"expireTimer": 86400,
"active_at": null,
"draft": "REDACTED",
"draftBodyRanges": [],
"draftChanged": false,
"draftIsViewOnce": false,
"draftTimestamp": null,
"draftAttachments": [],
"messagesDeleted": true
```


The only reliable way to delete this information is to delete all Signal app data, then re-register without entering the PIN or restoring data. This also deletes all contacts and messages.

Re-registering with the PIN recovers all contact metadata. From left and deleted groups, it appears to only restore group IDs, keys, icon colors, and some other items, but this is still potentially sensitive information.

Successfully registering an existing Signal account's phone number takes over or disables the account.

Signal uses SMS authentication. If a person's Signal account has registration lock disabled, an attacker who can observe or intercept their SMS messages can receive a Signal verification code to immediately take over their account. If registration lock is enabled, they can immediately deregister the person's device, making them unable to use their account. The attacker can then take over the account in 7 days if the person cannot re-register.

Once the attacker takes over, they receive all messages intended for their target, including group messages, and they can send messages from their account. Contacts see that their safety numbers have changed, but most people ignore these messages. After all, they may simply indicate that the person has reinstalled Signal. The account's name changes unless the attacker knows the previous name or guesses the PIN, but name changes are very common.

Additionally, deleting a Signal account does not delete it on the Signal servers for 30 days. If someone registers the number during this time, they can immediately access the account. Deleting an account leaves all groups, but they can still send and receive messages as the original user.

These design choices weaken the security and reliability of Signal accounts. Anyone can put a person's SIM card in another phone. Intelligence agencies intercept most or all SMS messages. Cell site simulators, SS7 attacks, and SIM swaps can also be used to intercept SMS messages.

ACIs are associated with phone numbers on the Signal servers, and they are difficult to change.

ACIs are unique 128-bit numbers that identify Signal accounts to other accounts and to the Signal servers. Accounts save the ACIs of all known accounts. ACIs are not shown in the Signal apps, and they are not mentioned on Signal's website, but they can be collected and tracked over time and between groups. People can also send messages to ACIs without any other information.

Signal's servers save ACIs with account phone numbers, so they can give account phone numbers to governments. According to an article by Micah Lee, "If Signal receives a government request for information about an account based on an active username, Signal will be able to hand over that account's phone number along with its creation date and last connection date." Looking up an active username simply provides the account's ACI, so it should be assumed that this is possible. It may have already occurred.

To obtain a new ACI, users need to delete their Signal account for 30 days or use a new phone number.

Other issues

Signal is centralized and runs on Amazon, Microsoft, and Google servers. These companies share massive quantities of data with intelligence agencies. They likely send Signal metadata to the US government, even though Signal probably does not. In addition, because Signal is centralized, it is easier to censor. Many governments already block Signal, and the US government could fully shut it down.

Notifications on iOS, Android, MacOS, and Windows give Apple, Google, and Microsoft the timing of messages. This does not happen on Linux and GrapheneOS.

The timing of message receipts from silent messages can be used to gain information about people's habits and devices. This is difficult to fully prevent, but the Signal developers do not have a plan to mitigate it. However, using Signal through Tor or a VPN likely reduces the accuracy of this attack.

Alternatives

These do not have all of the same features as Signal, and they are not as well-tested. Like Signal, they are not appropriate for all threat models.

Cwtch is a peer-to-peer encrypted messaging app which uses Tor to avoid surveillance and censorship. It does not require phone numbers, it is more metadata resistant than Signal, it has database encryption, it can use multiple accounts, and it functions with or without servers. It has not been independently security audited. The development team is small and could use support.

Briar is similar to Cwtch, but it also has basic blog, forum, and RSS reader features. It has received security audits, but it does not currently work on Tails or similar systems. In order to chat, two accounts require an exchange of links or QR codes.

Delta Chat is decentralized and does not require phone numbers. It is less metadata resistant than Signal, but it is easy to make new accounts. It does not have forward secrecy, so it is possible to decrypt multiple past messages with a leaked key. The developers plan to add forward secrecy and post-quantum cryptography in late 2026. It can be used with Tor, but UDP features such as calls and multi-client syncing cannot currently use Tor. Signal and most other apps face the same issue.

Other similar alternatives are not currently recommended, except for PGP email if it is necessary. Many other options are currently too experimental, not metadata resistant enough, or not trustworthy enough.

Signal suggestions

For those who continue to use Signal, these suggestions should be evaluated for each threat model. If anonymity and reliability are required, Signal is not the best option.

- Do not use Signal to organize or protest.
- Purchase a virtual phone number or a secondary phone plan to use only once for Signal registration. Continue paying for it or change numbers to avoid losing your account. This is not easy to do anonymously, but it is possible.
- Use GrapheneOS on a supported device. GrapheneOS is more resistant to data extraction tools like Cellebrite than other phone operating systems.
- Encrypt devices with long random passwords, and turn them off when they are not in use.
- Use Molly with database encryption.
- Use Tails, Orbot on GrapheneOS, or a trustworthy VPN. Note that VPNs are not anonymous, and using Signal calls with Tor may leak IP addresses.
- Verify safety numbers and identities, and treat safety number changes as possible account compromises.
- Avoid Signal groups with unknown people.
- Change your Signal settings to better options.

- Do not link additional devices.
- Make backup chats in Cwtch, Briar, or Delta Chat.

Further reading

The P.E.T. Guide: New Communication Infrastructure for Anarchists

Anonymous
Signal Problems
1 July 2026

Retrieved on 5 July 2026 from https://mtlcounterinfo.org/signal-problems/

theanarchistlibrary.org