LAW ENFORCEMENT GUIDELINES

These guidelines are intended for law enforcement authorities seeking information about surespot, llc accounts.

About surespot

surespot is the world's most secure military grade encrypted messaging app available today. Operating in over 100 countries with upwards of a half million users who have sent over 100 million secured messages. The surespot technology provides iron clad means for people to protect the content of their mobile communications with one another by using the industry's only zero-content system that is also backed and verifiable through a code base that is fully open source.

We don't collect any personal information about our users. Accounts are not associated to an email or phone number. We do not have plaintext copies of any messages. Communications are fully end-to-end encrypted and we do not hold the keys. From a technical standpoint, we have no ability to view, decipher or see plain text of any user data as it exchanges between devices.

Users can delete their messages at any time eliminating them from our servers and all of their contacts' phones.

surespot operates in an environment of total transparency and exists to protect each person's due right to privacy. We will cooperate with law enforcement only to the extent that the law requires.

Requests for Information

Any and all requests for user data requires a valid search warrant from an agency with proper legal jurisdiction over surespot.

Please address all inquiries and documentation electronically to surespot legal by emailing our attorneys at: legal@surespot.me

surespot will only respond to valid legal process issued in compliance with U.S. law. Non-public information about our company or users' accounts will not be released to law enforcement except in response to a court ordered grand jury subpoena, warrant or other valid legal proceeding that is supported by probable cause and delivered from an agency with proper jurisdiction over surespot.

We do not respond to foreign authorities as they do not have jurisdiction over U.S. companies.

We will never respond to a request voluntarily.

A Zero-Content-System

The pure simplicity of surespot's design and focus on core communication functionality is the reason why it doesn't need personally identifiable information from users. It is what we refer to as a "zero-content system". The app-related data we do collect is the base minimum amount required for the service and technology to function properly for the best user experience possible.

Because the content of communications are not available, our response to any requests for content will only reflect that it does not exist on our servers.

Notifying Users

Due to the security architecture of surespot, we don't know who our users are. We have no personal contact information that can be used to notify them. Personal contact information can be used to identify a person and/or possibly their location. For obvious reasons we don't want this, and neither do our users.

Limited Information

surespot stores the following data on its servers:

- Usernames
- Friend relationships (who is friends with who, blocked who, ignored who, deleted who)
- Conversation relationships (how many friends currently you have a "conversation" with - meaning have a sent or received a message with)
- Messages in the amount of MAX_MESSAGES_PER_USER (currently 1000) which each have a server timestamp, to username, from username, and encrypted content, or link to encrypted content (image or file)
- Encrypted message file data (image or other - anything but encrypted message content) is stored (encrypted in the same way text messages are) on rack space cloud files
- Total messages sent per user
- Total images sent per user
- Current message count per user. (How many messages they have stored in the database currently, will always be <= MAX_MESSAGES_PER_USER (currently 1000))
- Signing (DSA) public keys and versions
- Encryption (DH) public keys and versions
- Encrypted "friend images" or avatars and friend aliases that are assigned to certain usernames. These are encrypted with a key generated from ECDH key derivation of assigning identity's private/public key-pair
- Google GCM id (used for push messaging) which is related to the username in the surespot database
- Apple APN token (used for push messaging) which is related to the username in the surespot database
- If voice messaging is purchased, a purchase token given to us by Google or Apple which is related to the username in the surespot database
- Server logs may contain any of the above information and are in a 20 log - 5MB per log rotation

Requests for Data Must Include

- Law enforcement letterhead
- A valid official return email address and point of contact
- Search warrant, subpoena or other valid court order for information
- User name for account being investigated
- Date of request
- Account information being sought

Records Authentication

The records that we produce are self-authenticating. Additionally, the records are electronically signed to ensure their integrity at the time of production. If you require a declaration, please explicitly note that in your request.

Mutual Legal Assistance Treaties

surespot's policy is to promptly respond to requests that are issued via U.S. court either by way of a mutual legal assistance treaty ("MLAT") and letters rogatory, upon proper service of process.

Contact Information

surespot, llc.
2995 55th Street
#18034
Boulder, CO 80308
legal@surespot.me

Non-law enforcement requests should be submitted through via email to support@surespot.me