# SafeTalk Encrypted Messenger

## *A new paradigm in messaging*

The latest generation of end-to-end encrypted messengers boasts “privacy” and then ask you to accept around 30 dangerous permissions. Then they make you identify yourself. Stop right there. That is the opposite of privacy. They know who you are and they know everything about you.

Fortunately that is now all in the past for now there exists a safe messenger you can trust.

If you have read the SafeTalk high level overview and the linked documents then you have an understanding of SafeTalk. If you haven’t done this, please have a look.

SafeTalk is very different from other messengers. It runs in a virtual isolated environment on your Android device. It can’t see your contacts, your videos, your pictures, your SMS messages, it doesn’t know where you are, or know your browsing history, or where you go, or who you call. It doesn’t even know the IEMI of your phone.

SafeTalk is kept completely in the dark when it comes to both you and your phone. The beauty of this is that it can’t tell anybody anything about you or your phone. This is all enabled through having virtually no Android permissions to look at anything on your phone.

All SafeTalk can do is send and receive end-to-end encrypted messages.

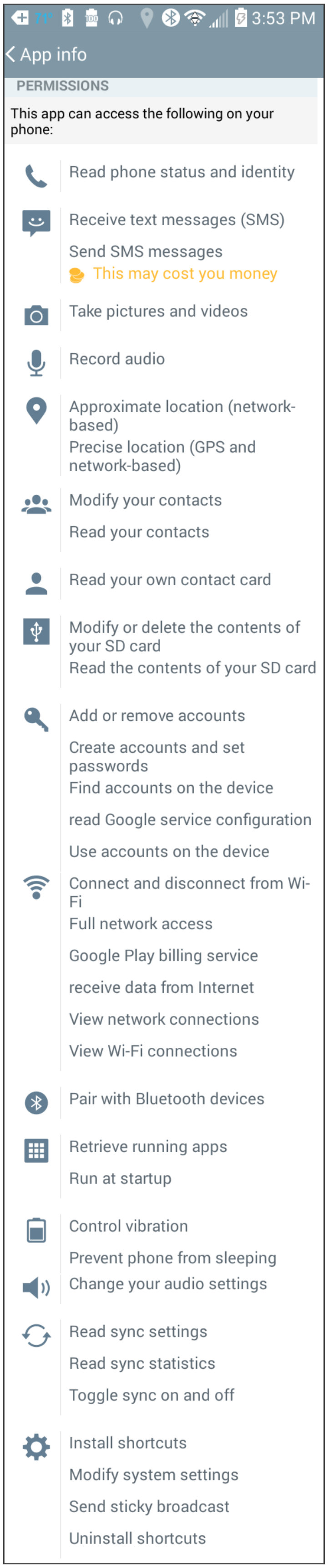
This is an actual SafeTalk message that travels through Google Cloud Messaging . . .

{"Message":"b4BUIVQSX4w4qsAYMt8O7/gY+aJ1liddtg0qcaoguAIj+1GPTdjSu5nHUcKIY9GQ\n","aeskey":"VpC8gtQ5LaPVUAWZT3CK5KtiSqktPa/yw2vRnZ7d9EYEc0I5M+xVRiP6lF0/iQ8Fgmw7thgqdjjCDhVz5im/PQCEwxmZPmG6WCQK1eNxkNcm8TtsntH1asxBAqW+mzcMl2r0eH6H2EqD7p0Z3MlMrKGbxLKjwvJrjFH3xgBIOK5jkGfS7Xyx0cIFr7hkmtUEMhYTUH+xjDsgsBmr+zDhDMzWVeoVQG3GAkLGd0lNSQHJzrMKr1nQYDtqOzVoEMbBPlVeslxedQtyu07SkjzclYxwTTkD0oqA9UDAYYsOcYOzyKuiAG9CpW1jS2n2kItNAuqWFflQYYzbd1IvO6V8+w\u003d\u003d","fromLang":"DtqOzVoE","fromPhoneKey":"hgqdjjCDhVz5i","fromUsername":"MrKGbxkGfS7","mine":"y","subActive":"n","timeSentGMT":"gtQ5LCQK1","toPhoneKey":"WVeoVQG3GA","tran":"##03"}

If you read on, you will understand that our encryption is fail-safe. Nobody is going to be breaking this encryption.

As of March of 2017 SafeTalk is out of Beta. It is running only on Android devices at this time. It works with a single sender and receiver. It’s not for chatting with all of your Facebook friends. It’s designed for serious and secret communications between two people who trust each other. It is as safe as whispering in someone’s ear in the middle of the desert.

WhatsApp permissions . . .



3:53 PM

< App info

PERMISSIONS

This app can access the following on your phone:

Read phone status and identity

Receive text messages (SMS)
Send SMS messages
This may cost you money

Take pictures and videos

Record audio

Approximate location (network-based)
Precise location (GPS and network-based)

Modify your contacts
Read your contacts

Read your own contact card

Modify or delete the contents of your SD card
Read the contents of your SD card

Add or remove accounts
Create accounts and set passwords
Find accounts on the device
read Google service configuration
Use accounts on the device

Connect and disconnect from Wi-Fi
Full network access
Google Play billing service
receive data from Internet
View network connections
View Wi-Fi connections

Pair with Bluetooth devices

Retrieve running apps
Run at startup

Control vibration
Prevent phone from sleeping
Change your audio settings

Read sync settings
Read sync statistics
Toggle sync on and off

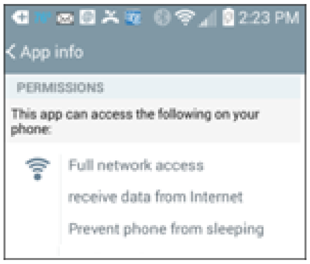
Install shortcuts
Modify system settings
Send sticky broadcast
Uninstall shortcuts

#1

SafeTalk can't steal data from your phone

The other apps certainly can

SafeTalk permissions . . .



2:23 PM

< App info

PERMISSIONS

This app can access the following on your phone:

Full network access
receive data from Internet
Prevent phone from sleeping

This illustration uses WhatsApp as an example because it's representative of the kinds of permissions other messaging systems use.  Our Permissions Document also compares SafeTalk permissions to those of Signal Private Messenger.

The permissions you see for SafeTalk are all that is really needed for an end-to-end Encrypted Messenger app.

If you understand Android permissions you know that your data is safe with SafeTalk.  It’s not a matter of trusting what we say.  If an app doesn’t have permissions to get at data then it is impossible to get at the data.

## #2
## SafeTalk has superior encryption

WhatsApp just got around to adding "static" encryption on some of its messages in November of 2014. With WhatsApp, encryption was an afterthought.

By "static" encryption we mean that the seed and the encryption algorithm are constant. This means that, for instance, if the NSA Quantum computer breaks their encryption, the NSA will be able to decipher all the messages sent through their app.

If that same NSA Quantum computer breaks the encryption in a SafeTalk message, they will only be able to decipher that one message because Safe Talk's encryption key changes on each message.

Later on we describe exactly how this is done.

## #3
## SafeTalk messages are untraceable

Anyone familiar with the NSA PRISIM program has seen the U.S. Government force tech companies to turn over data on their servers about the general public without any individual warrants.

None of this can be a problem for messages sent using SafeTalk because a SafeTalk message leaves no trace anywhere on the internet or in any clouds or servers. So, if the NSA demanded Dean Blakely & Assoc. to turn over messages for our users, it would be impossible for us to comply. SafeTalk users can easily delete messages sent and received from their phone leaving no trace anywhere in the universe.

In 2013, information leaked by Edward Snowden showed that Skype had a back door which allowed Microsoft to hand over their users' messages to the NSA despite the fact that those messages were officially end-to-end encrypted.

SafeTalk doesn’t keep any messages to hand over. Also, if you go to www.deanblakely.com you will see that we post a Canary Warrant.

The first thing you must do upon installing WhatsApp or TextSecure is to give them your real phone number. You have now been identified. This means that any data or metadata taken off your phone or messages can be linked to you. This makes the data much more valuable on the marketplace.

#4

SafeTalk lets you remain anonymous - if you want

Hangouts want's your Google Group account number. SnapChat wants your account email address.

With SafeTalk you *NEVER* have to identify yourself. No phone number. No email address. No Google Account credentials. No nothing. You must register with SafeTalk but you do it with a user name of your choosing. If you want, you can enter your real name or you can enter "ILoveCats" or anything else you want.

SafeTalk is the only messaging system on the planet where you can remain totally anonymous.

You can also have multiple identities. Some public, some private - however you want them.

#5 SafeTalk translates language

Nobody else does that!

When you register you indicate what language you speak. The rest is automatic. You will always get your message in that language.

Now, for the first time, people who speak different languages can message with each other. This feature might be less valuable for typical Americans who never interface with anyone who doesn't speak English. For people in smaller societies who might want to communicate to more diverse groups it may be very useful.

# How to use SafeTalk . . .

You first need to register as a user in order to use SafeTalk. When you register you make up a User Name that must be unique among all SafeTalk users. You can enter your real name or, if you want to remain anonymous, you can enter some secret name.

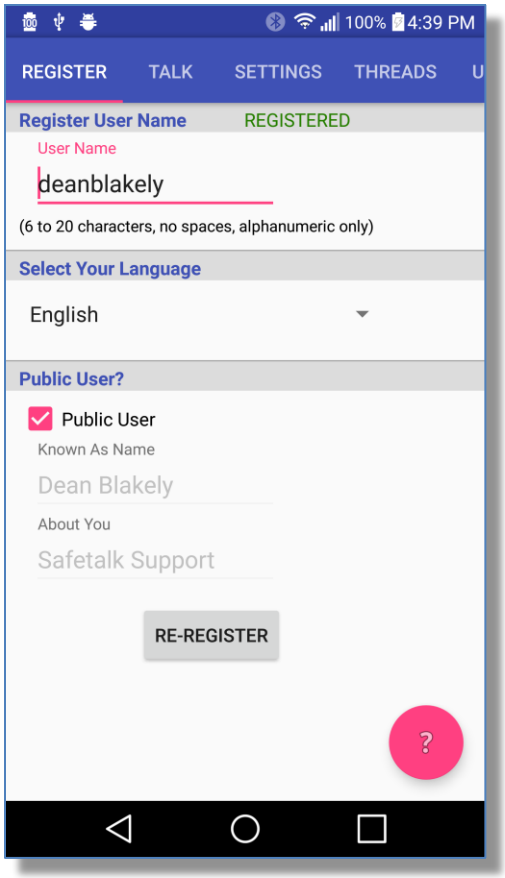
You also have a choice between being a public or private user. Public users are seen by everyone who uses the app. These are people who are, in essence, inviting everyone to talk with them. I, Dean Blakely, am a public user because I support the app. You become a public user by filling in Name and About fields and checking "Public User".

The vast majority of SafeTalk users will want to be private users and be known only to a limited population of their correspondants.

You can re-register anytime changing your status or User Name.

Both public and private users can be anonymous - or not.

As you can see, SafeTalk correspondents are separate and unrelated to your Contacts. SafeTalk does not have permission to read your Contacts.



Register User Name REGISTERED

User Name

deanblakely

(6 to 20 characters, no spaces, alphanumeric only)

Select Your Language

English

Public User?

☑ Public User

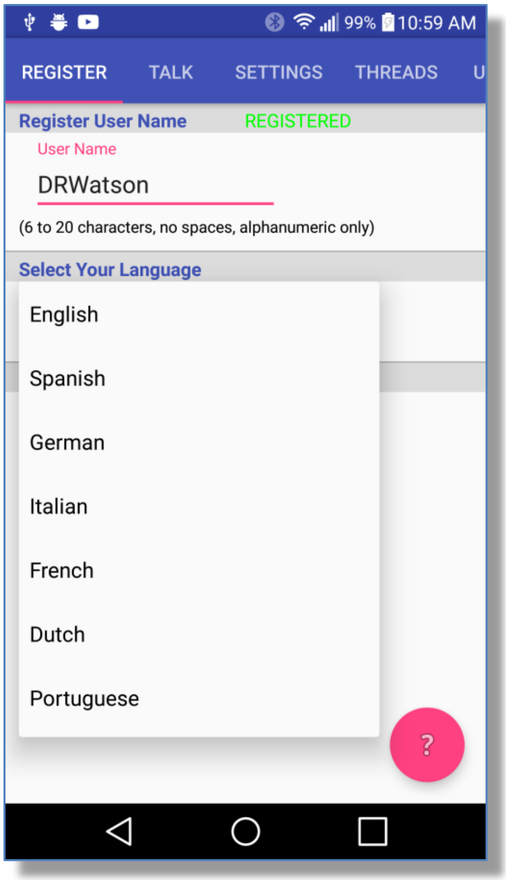
Known As Name

Dean Blakely

About You

Safetalk Support

## Automatic Message Translation . . .



Register User Name REGISTERED

User Name

DRWatson

(6 to 20 characters, no spaces, alphanumeric only)

Select Your Language

English

Spanish

German

Italian

French

Dutch

Portuguese

When you register yourself with SafeTalk you specify the language you would like to receive your messages in. The initial version of SafeTalk supports the eight languages you see in the screen shot nearby.

SafeTalk uses both the Microsoft Translator and the Google Translator. Future versions of SafeTalk will support many more languages.

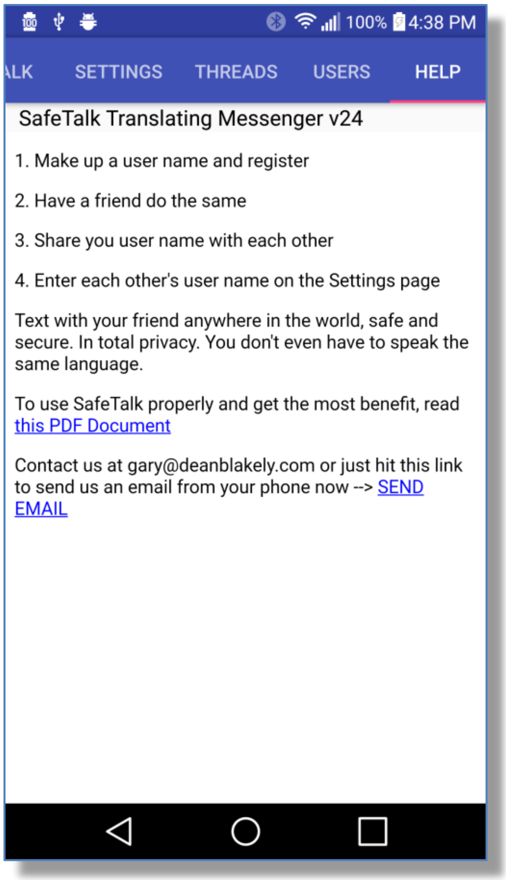
Both Microsoft and Google charge us for the translations you make so we need to pass that cost on to the user of the app. When you first download SafeTalk, you get 10,000 characters of translation for free. Beyond that you need to purchase additional translation credits at a very low price. This is done on the Settings Page.

**Security Caution:** The Microsoft/Google translation servers "see" the plain text. But they don't know who it is coming from - they just know it is coming from the SafeTalk app. So, using the translation feature might reduce message security to some extent. Both companies claim not to retain nor share translated messages with anyone.

The help page tells how to use the app it in the simplest of terms. At least two people have to decide to start using SafeTalk at the same time. You both download the app, share your private name with each other and begin messaging.

No one else in the world will know you are messaging or what you are saying. There is no messaging app on the market that provides that level of privacy.

Alternatively, you could just try talking to public users to get used to using the program. Or become a public user yourself. Nothing is permanent as you can always re-register as you wish.



SafeTalk Translating Messenger v24

1. Make up a user name and register

2. Have a friend do the same

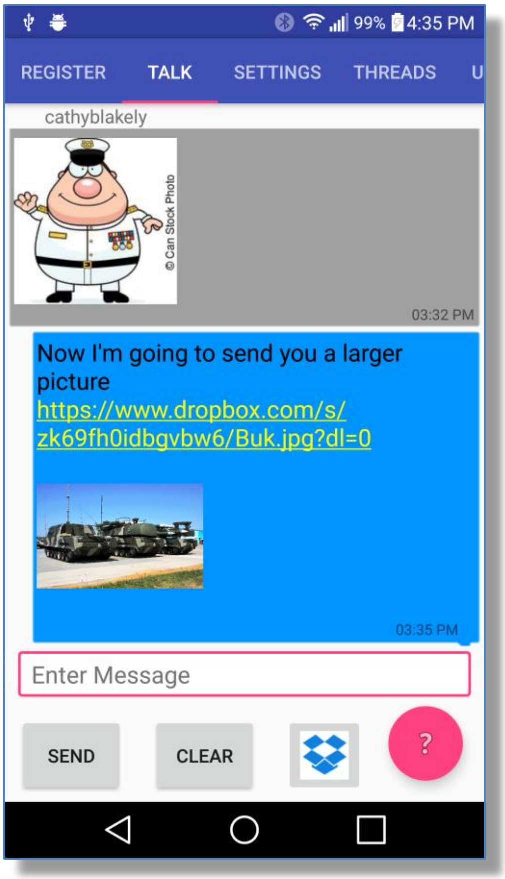
3. Share you user name with each other

4. Enter each other's user name on the Settings page

Text with your friend anywhere in the world, safe and secure. In total privacy. You don't even have to speak the same language.

To use SafeTalk properly and get the most benefit, read this PDF Document

Contact us at gary@deanblakely.com or just hit this link to send us an email from your phone now --> SEND EMAIL



cathyblakely

03:32 PM

Now I'm going to send you a larger picture https://www.dropbox.com/s/zk69fh0idbgvbw6/Buk.jpg?dl=0

03:35 PM

Enter Message

## Failsafe multimedia transport . . .

SafeTalk does not have access to your multimedia content on your phone. Valuable content shouldn't be on your phone anyway - it should be in a cloud somewhere so when you drop your phone in the toilet you won't lose any content.

There is a built in Chooser button for Dropbox which is the only cloud service we know of that allows password protection. We don't allow packaging multi-media objects into the actual message for good reason. (1)

It is understood that, unless you use Dropbox, this is more cumbersome than other messaging apps that just pick up the object directly from your phone but the payoff is security and efficiency.

To include a link to a multimedia object in Dropbox, use the Dropbox chooser button to select the object then hold down your finger on the textbox. You will see a "Paste" popup that you hit to embed the link into the message.

To include a link from another internet source you will need to get that link into the clipboard before you send the message and then paste it in the same way as above.

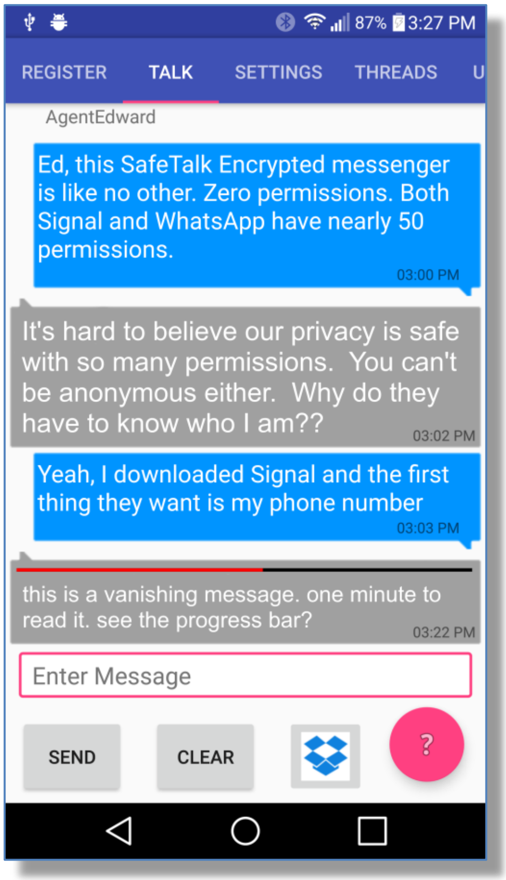
## How communication works . . .

To talk with a private user, you need to know their User Name and you both need to be registered. The person starting the conversation enters his/her correspondent's User Name on the Settings page in the "Correspondent username" box. If there is no such user, you will be immediately informed. To talk with a public user, just select them on the Public Users page.

At this point you can enter a text message on the "Talk" page, hit send, and the receiving phone will get the message - usually within a few seconds. If your correspondent is not using SafeTalk at the time, they will get a SafeTalk Android notification the next time their phone is turned on. If they are using SafeTalk but are having a conversation with another SafeTalk user, they will get a toast message informing them that they have received a message from you. It all acts very much like SMS texting.

The SafeTalk maximum message size is 320 characters.

To send a vanishing message, hold the send button down instead of just hitting it. You will receive a confirming toast that it was sent in vanishing mode.



AgentEdward

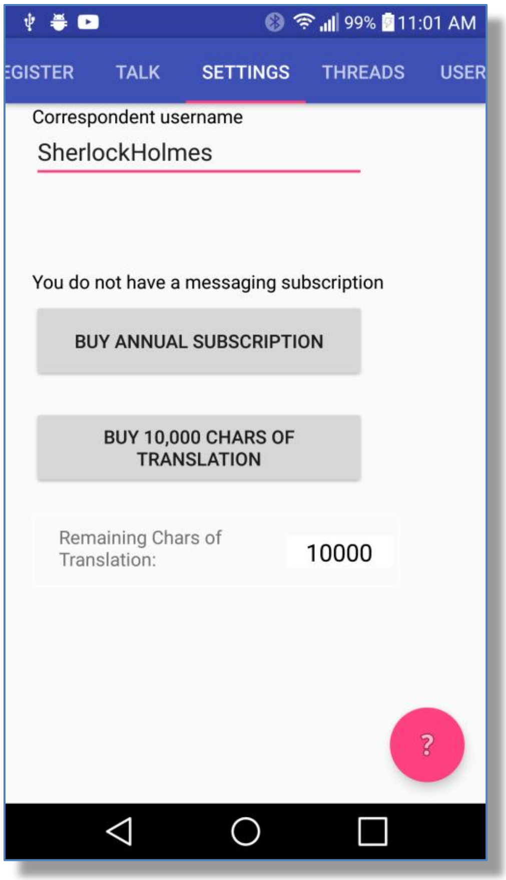
Ed, this SafeTalk Encrypted messenger is like no other. Zero permissions. Both Signal and WhatsApp have nearly 50 permissions. 03:00 PM

It's hard to believe our privacy is safe with so many permissions. You can't be anonymous either. Why do they have to know who I am?? 03:02 PM

Yeah, I downloaded Signal and the first thing they want is my phone number 03:03 PM

this is a vanishing message. one minute to read it. see the progress bar? 03:22 PM

Security Caution! Using Android's speech recognition sends your voice message to the Google servers. So if you need absolute privacy you should type your messages.



Correspondent username

SherlockHolmes

You do not have a messaging subscription

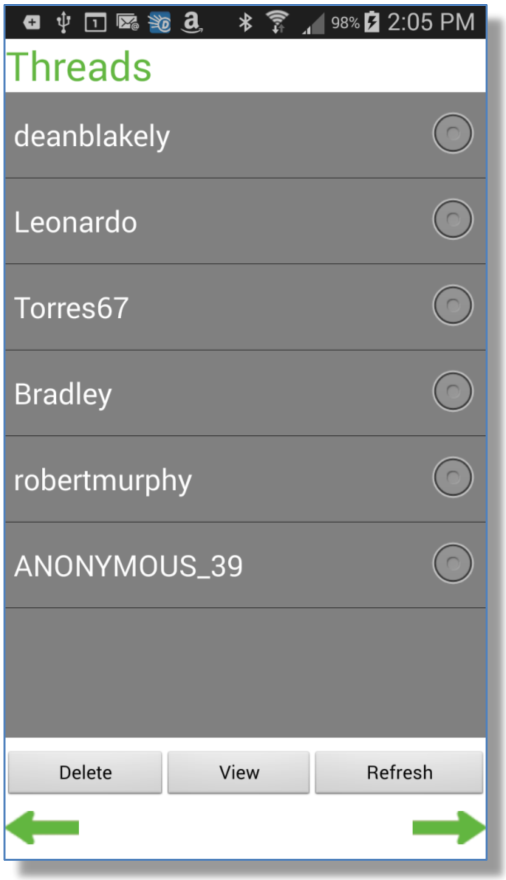
Remaining Chars of Translation: 10000

## Free for light use, low cost for heavy use . . .

We need to charge a fee for heavy use of messaging because we need to maintain cloud servers that service the traffic. An unlimited messaging subscription is currently one U.S. Dollar per year. Without the subscription, you can still send several messages a day.

If you need to use translation . . .
Both Microsoft and Google charge us for the translations you make so we need to pass that cost on to the user of the app. When you first download SafeTalk, you get 10,000 characters of translation for free. Beyond that you need to purchase additional translation credits at a very low price.

If you have zero translation credits, the messages will always be displayed in the language they were sent in.



We need to charge something because we don't make any money stealing your data and selling it.

## Threads . . .

By default, all conversation threads are saved on the phone under the correspondent's User Name.  If you hit the view button on the Threads page, the thread for the selected User Name will be restored to the Talk page.  You can Clear a thread or Delete a thread whenever you want.

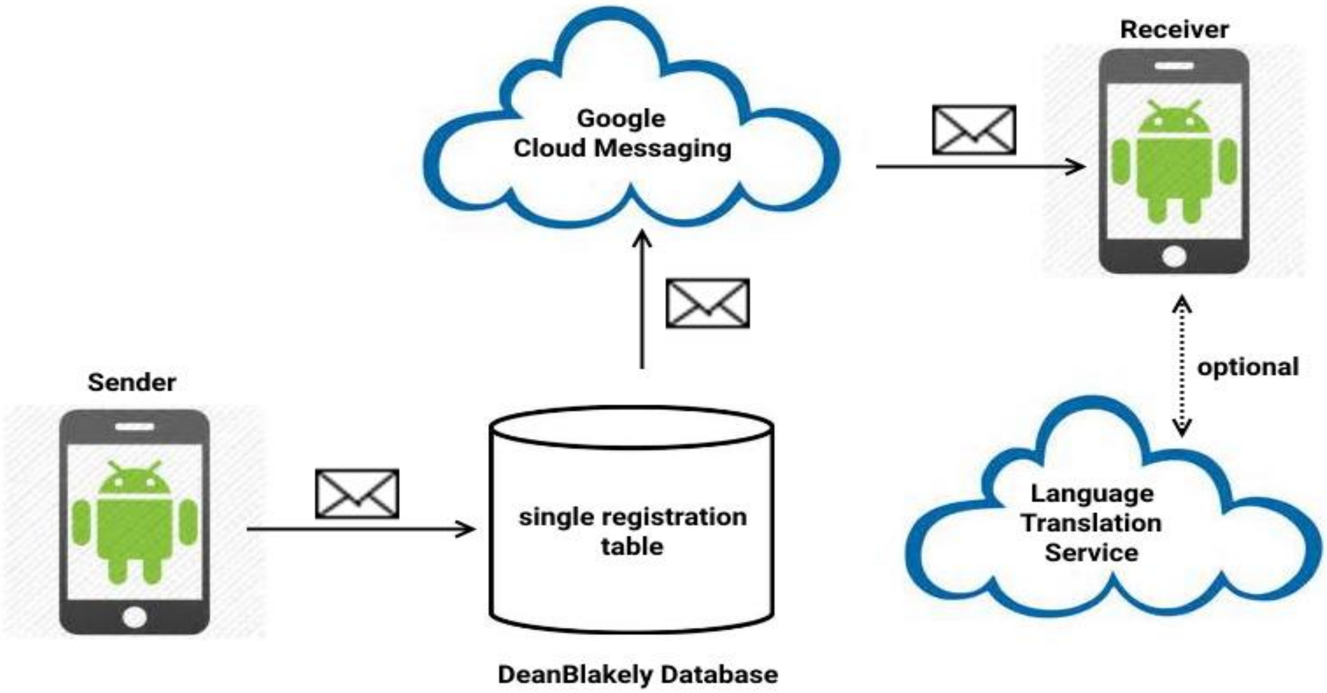
## Limitations as of March 2017. . .

Group distributions are not yet implemented.

Communication is limited to Android phones only.

# How it Works - Proof that it's Safe

Having read the above sections you know exactly what SafeTalk does along with the privacy and anonymity it can provide.  This section discloses more about how it works.  The app is brand new having less than 300 users at this writing.



**How can you trust what we actually do in our code?:** We expose all of our source code to you from the actual .APK file you are running.  You can have any intermediate level Android developer examine our code and tell you exactly what we are doing.

Because we need to be completely transparent to our users, we do not obfuscate our source code.  This means that you can upload your SafeTalk.apk file to your computer an go to http://www.decompileandroid.com/ where you can receive a decompiled zip file containing all of the source for the application.

We are not worried about anyone stealing our code because the heavy lifting code is all done on our server.  All you should really want to be concerned with is (1) your plain text message isn't going anywhere except to your correspondent and (2) our encryption is doing what we claim.

We even have another PDF here that documents what we do to make the job easier for the developer doing the audit.

This is much better than "open source" because you are seeing the source code from the actual .APK that you are running.  With open source you can see source code on a server and download it but it didn't come from the actual .APK you are running.  Trying to determine that the open source code all lines up with what you are actually running is a huge task that nobody actually ever does.  Your APK may have a backdoor in it that is not in the source code.

This transparency along with the minimal Android permissions constitutes proof that SafeTalk is the safest and most transparent messenger in the world.  No messenger on the planet is this safe.

**Encryption:** SafeTalk uses both symmetrical AES encryption and asymmetrical RSA encryption. When a user registers, a public key is generated that gets published in our server database. A private key is also generated that gets stored in their phone and never goes to any database anywhere. When a correspondent is selected, their public key is obtained on the sending phone. Before a message is sent, the text is encrypted by AES using a random AES key. The AES key is then encrypted using the correspondent's public RSA key. Both the encrypted AES key and the encrypted message go down the line to the receiving phone where the correspondent uses their private RSA key to decrypt the AES key which is then used to decrypt the message. AES 128 bit is used instead of AES 256 because it's much faster and more appropriate for cell phone processors.

If a user want to be issued new public and private RSA keys they can go into Android settings and clear memory for the app. The next time it runs they will be issued new keys.

This means that the AES symmetrical key is different for every message and that we are “double encrypting.” So if the NSA figured out how to crack the encryption in a SafeTalk message they would only have that one message. The next one would have a different AES key.

**DeanBlakely Database:** Every user must register before using SafeTalk using any user ID they can makeup but it must be unique to all other SafeTalk user IDs. The database consists of only one table containing their phones device id (the key), User ID, GCM registration number, and the language they want to receive their messages in. Actual messages nor message metadata is never retained in any database. A user can change his user ID as often as desired. Therefore Dean Blakely & Assoc. could not possibly comply with, for instance, an NSA warrant for any kind of data because we don't keep it.

**Communication method:** All communications are done using HTTP POST. SMS is never used.

**Google Cloud Messaging:** GCM gets the encrypted message along with the GCM registration ID of the receiving phone. GCM therefore knows what phone this encrypted message is going to but it does not know what phone the message came from or who sent the message. If Google turned all of this data over to the NSA, it would be useless to them as they don't know how to get the seed. If they somehow found the seed, it would be good only for that single message. GCM *does* retain the encrypted message, for a limited amount of time, until it successfully delivers it to the receiving phone.

**Identity Assurance:** The sections above describe public, private, and anonymous user IDs. Identity assurance naturally occurs if you keep your user ID a secret. So, for instance, if you and a friend swap your user IDs and neither of you tell anyone else, you can have secret communications forever. If you become a public user or share your user ID with many other people then there will be no identity assurance at all. It's your choice.

**Language Translation:** This is a nice feature that may catch on in smaller countries but it compromises message security because the message is sent to Bing Translate or Google Translate) in plain text after it is decrypted on the receiving phone. So, where absolute privacy is a must, it shouldn't be used. Bing and Google say they don't retain or share any of this data.

**Any questions or other communication should be sent to gary@deanblakely.com**

**Footnote. . .**

**(1)** Multimedia attachments are big and getting bigger as technology improves resolution. It's very ineffective to embed a MMS object into a message and worse if the message goes to multiple correspondents. Imagine sending a large video to 100 people when only ten of them would ever watch it. Also, encrypting and decrypting large attachments takes a lot of computing and battery power from phones.

If you want to send an attachment,  it's best to put it in a cloud repository such as Dropbox, where it is safely encrypted, and put the URL to the attachment in the text - which gets encrypted.  If you password protected the object in the cloud, you simply tell your correspondent what the password is in the text.

END OF DOCUMENT