Mobile App User Manual

Pryvate

Powered by Criptyque

Table of Contents

Overview	1
Operator Screen	2
Secure Voice Service	2-3
Establishing a trust relationship	4
Removing a trust relationship	4
How to make a call via Contacts	5
How to bring up the keypad during a call	6
How to mute the audio during a call	6
How to receive a call	7
How to put a voice call on hold	7
Secure Video Service	8
How to initiate a video call	10

Secure Conference Calling Service 11

How to initiate a secure Conference Call 12

Secure Instant Messaging Service 13

How to initiate a Secure Instant message 14

Using Contacts Section 15

Managing Contacts 16

Using the Recents Section 17

Troubleshooting 18

Email User Manual 19

- Pryvate Email Client 20-23
- Log into Pryvate Email 24
- Composing an Email 25-26
- Reading an Email 27

Added Security (Android) 28-30

Added Security (iOS) 31-34

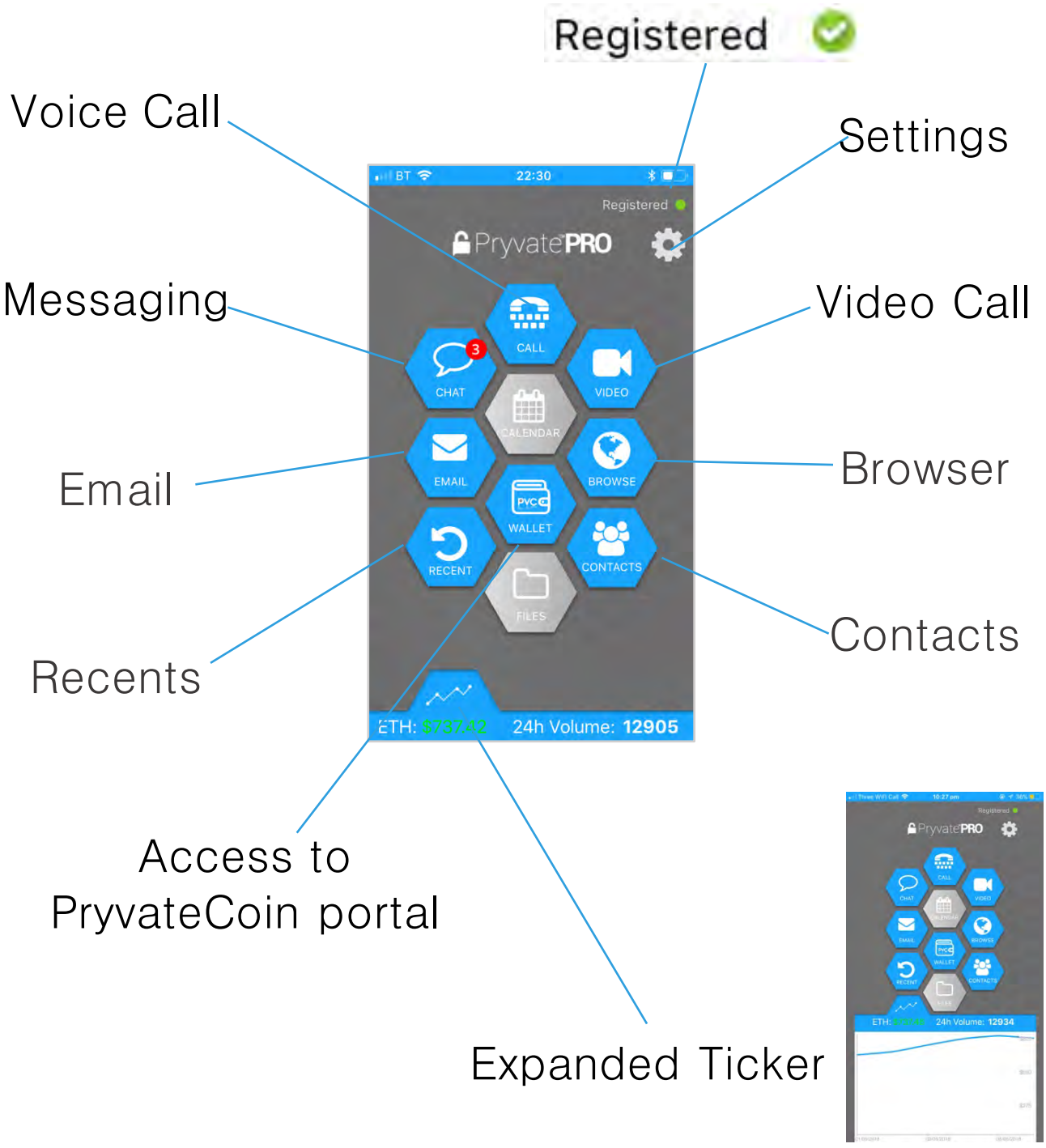
Overview

Pryvate is the most secure voice, email & chat app for business people & individuals that require a high level of communications encryption to protect their sensitive data, pictures and calls.

An all-in-one voice, email, video calls, messaging & picture sharing app.
Feel at ease with a military grade communication encryption technology.
Establishes direct trust relationships with no server or middleware.

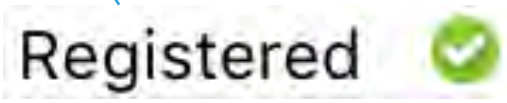
Download the app and setup your Complimentary Trial account at pryvatenow.com.

Operator Screen



New Operator screen providing easy navigation throughout the app.

Secure Voice Service

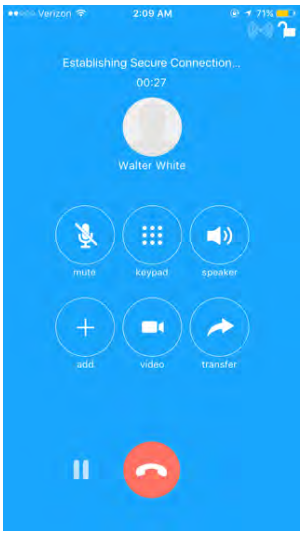


Once your service is active you will see a green “Registered” symbol at the top of your device and also you can open your app. Once you open the app you will see the main dialer screen. If you know the Pryvate subscribers number to be dialed then simply dial it and click the telephone button to make the call. Simply dial as an international entry.

You need to enter their number including country code, and the + (plus) symbol, you can enter the + (plus) symbol by holding down the 0 (zero) button. For example in the UK it is +447888 123456 and the US would be +1 XXXXX XXXXXX etc.

All US subscribers must put the "+1" country code before dialing a domestic US number, even when dialing in the US, for example: the number (555) 555-5555, should be dialed as +1 555 555 5555

Establishing a Trust Relationship

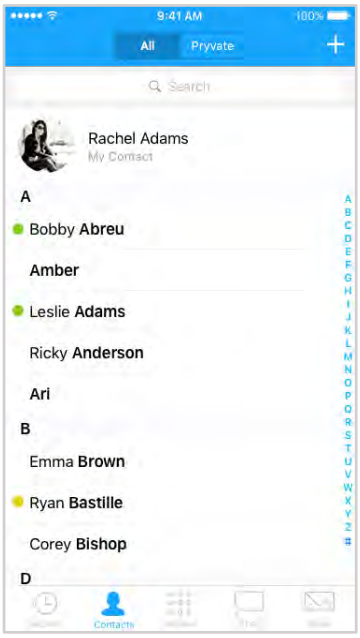


The padlock in the upper right corner will lock. You only do this the first time you call another Pryvate user, but if you wish to see the SAS Pass Phrase and want to re-establish your trust relationship, hit the Lock symbol in the top right.

Removing a Trust Relationship

To remove a trust relationship hit the lock symbol in the upper right and “deny” the peer relationship

How to make a call via Contacts

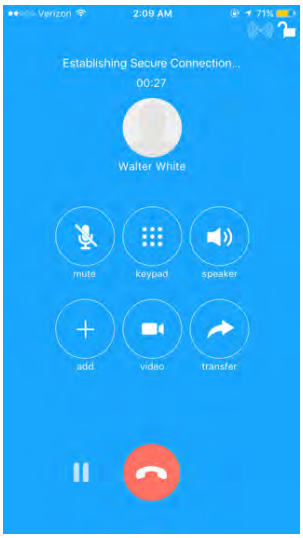


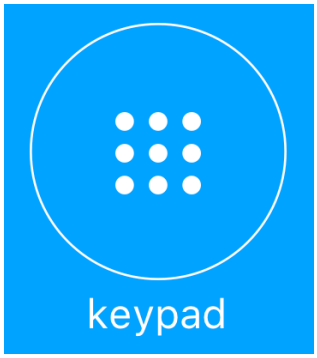
If it is to a former trusted Pryvate number and it is in your contacts then select the contact and press the call button . Note when you subscribed your number is secured through the app.

Your normal number is your secure number. You just need to let users know you are Pryvate and to make sure they use your number in international format.

Your Pryvate contacts must have international pre-fixes so that you can dial them automatically.

How to bring up the keypad during a call

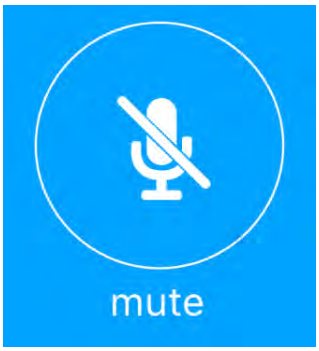




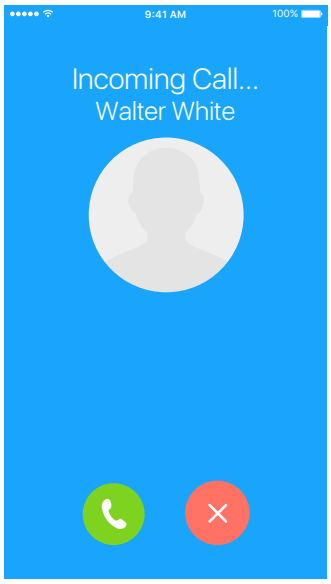
Tap the keypad button on the top row or follow your devices instructions.

How to mute the audio during a call

Simply press the microphone icon on the top row to mute/unmute



How to receive a call

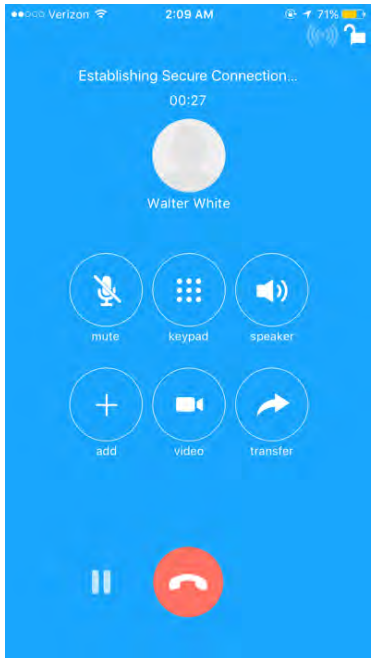


When receiving a call simply hit the green answer button.

To decline click the red "x" button.

How to put a voice call on hold

Press the pause icon on the bottom left. The person on the other end will hear music or silence depending on the handset you are using. You will see a play icon. To take the caller off hold press the play icon.

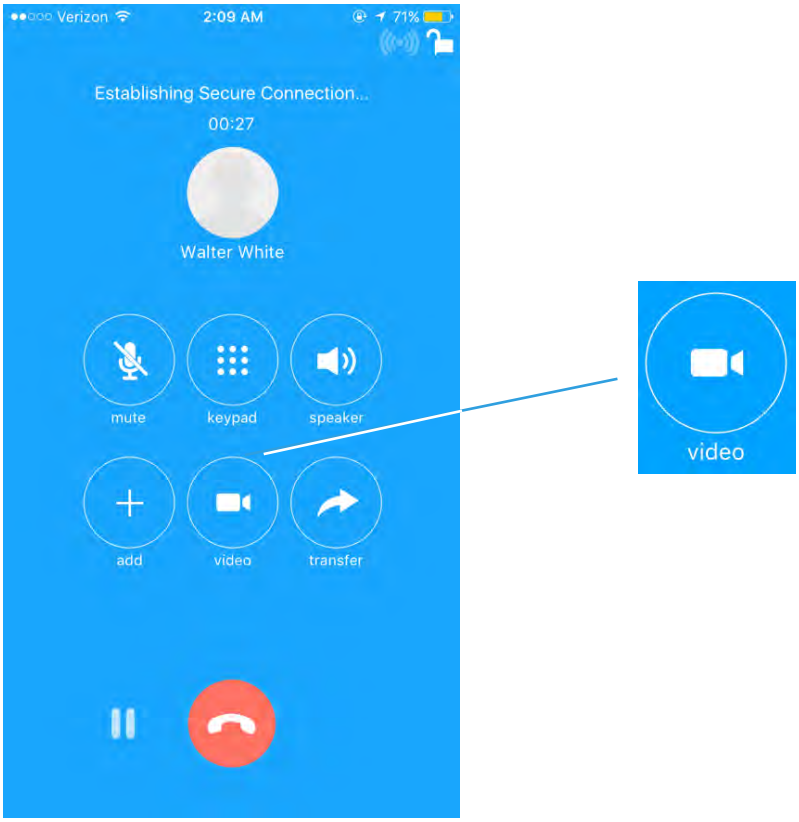


Secure Video Service

As soon as you can make a secure voice call to another Pryvate user, you will also be able to make a video call the same user. If you know the Pryvate subscriber's number, simply dial it and click the telephone button to make the call. Simply dial as an international entry. You need to enter their number including country code, and the + (plus) symbol, you can enter the + (plus) symbol by holding down the 0 (zero) button. For example in the UK it is +447888 123456 and the US it would be +1XXXXX XXXXXX etc. This procedure is the same as making a normal Secure voice call.

How to initiate a video call

Once a voice call is initiated you can then switch to video by pressing the video button. As per a voice call you can mute the video call. Note the codecs are designed to be of the best quality. If you are experiencing low quality video the most likely cause is low bandwidth on your internet connection.

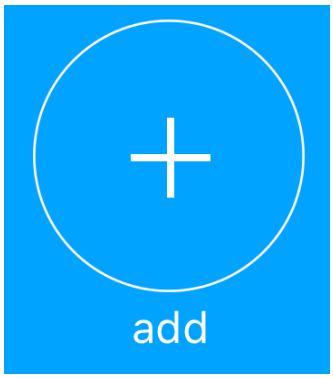


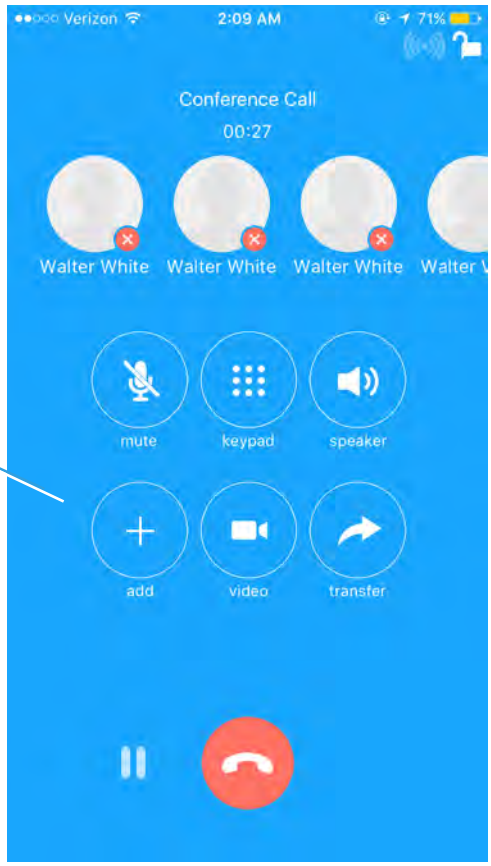
Secure Conference Calling

As soon as you can make a secure voice call to another Pryvate user, you will also be able to make a conference call, by adding other Pryvate users to the current call. If you know the Pryvate subscribers number to be dialed then simply dial it and click the telephone button to make the call. Simply dial as an international entry. You need to enter their number including country code, and the + (plus) symbol, you can enter the + (plus) symbol by holding down the 0 (zero) button. For example in the UK it is +447888 123456 and the US it would be +1XXXXX XXXXXX etc. This procedure is the same as making a normal Secure voice call.

How to initiate a secure conference call

Click the “+” add button to add a new caller. To remove a caller from the conference click the ⊗ over the participant’s avatar. The amount of callers on your conference call is limited to your devices computing power. Virtually all handsets can handle 3 callers.





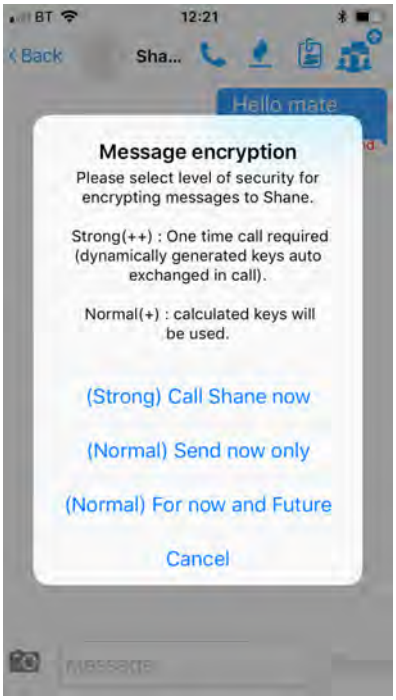
Secure Instant Messaging Service

As soon as you can make a secure voice call to another pryvate user, you will also be able to send secure Instant Message to that Pryvate user. However if no call has been made to recipient Pryvate user, you will be asked to select level of security for encrypting messages;

Strong(++) : One time call required (dynamically generated keys auto exchanged in call)

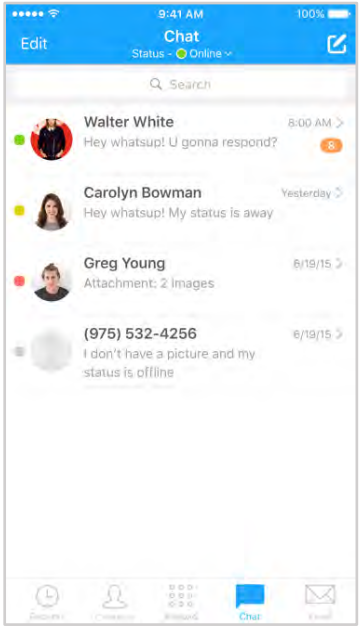
or

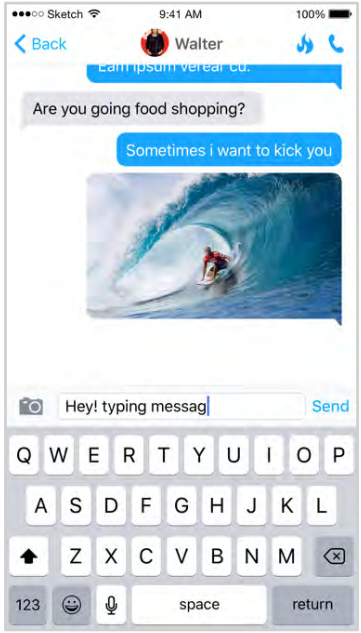
Normal(+) : calculated keys will be used. With normal you also get the choice to send now only or for future messages too..

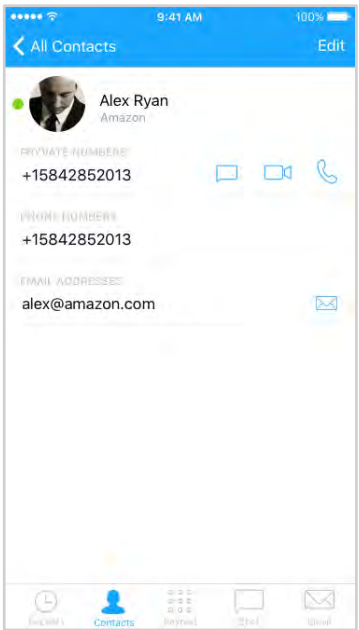


How to Initiate a Secure Instant Message

After your selection of Message encryption level (see previous page) to recipient Pryvate user, they can receive and send if they are connected to the internet. No different to using SMS on a mobile phone. From the chat tab you can select from existing converations or start a new conversation by clicking the new chat button in the upper right. Or from contacts select the chat button

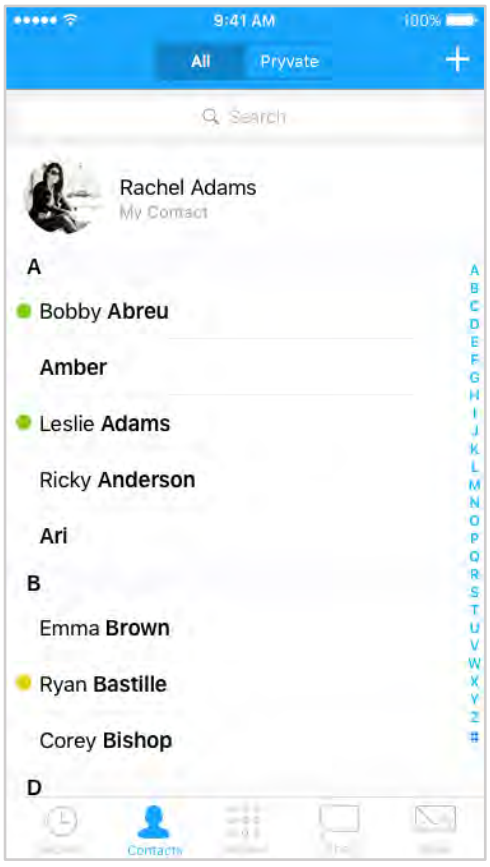


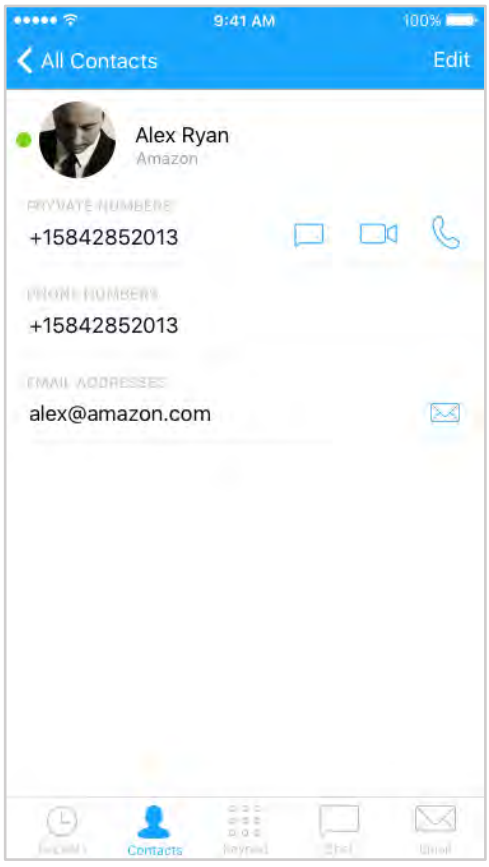




Using the Contacts section

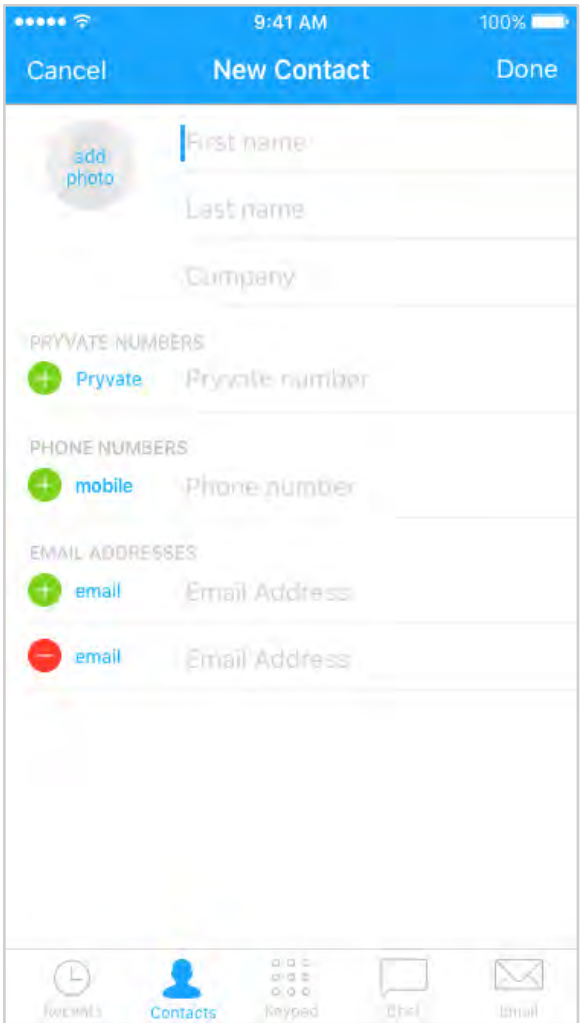
The contacts section is available by pressing the contact button located on the bottom menu. All of your iPhone or Android contacts will be listed here. You can toggle between ”All” contacts and “Pryvate” contacts on the top bar.

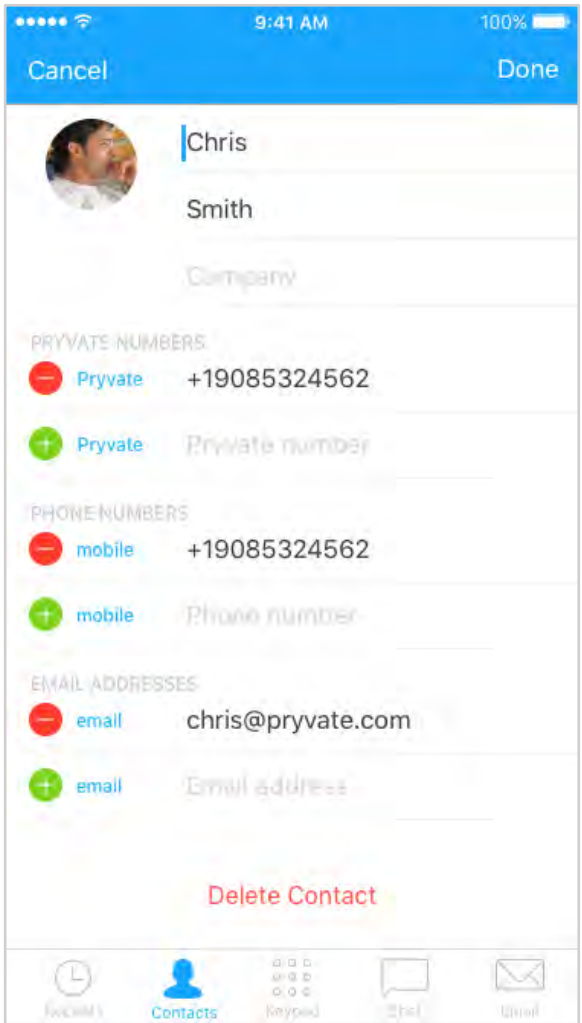




Managing Contacts

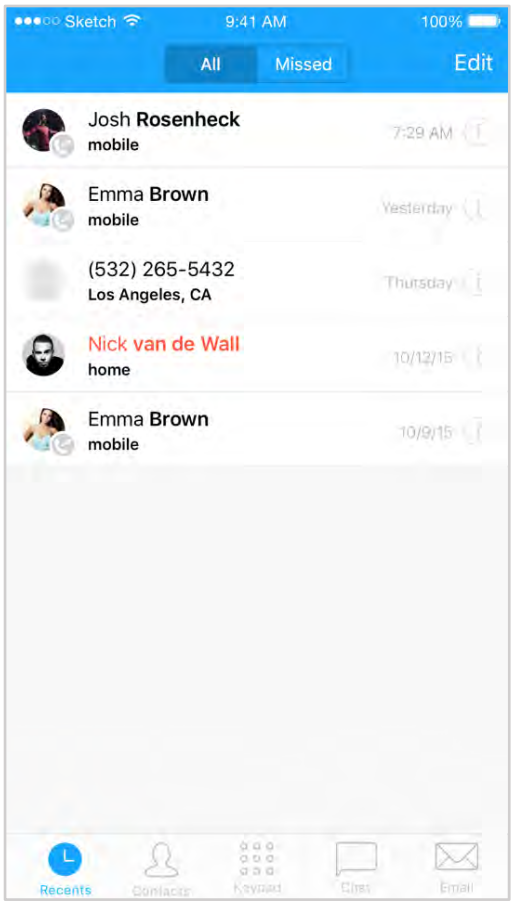
You will also be able to initiate secure voice calls and secure Instant Message to that Pryvate user listed in contacts directory. Like all contacts directories, you are able to add, edit and delete entries.

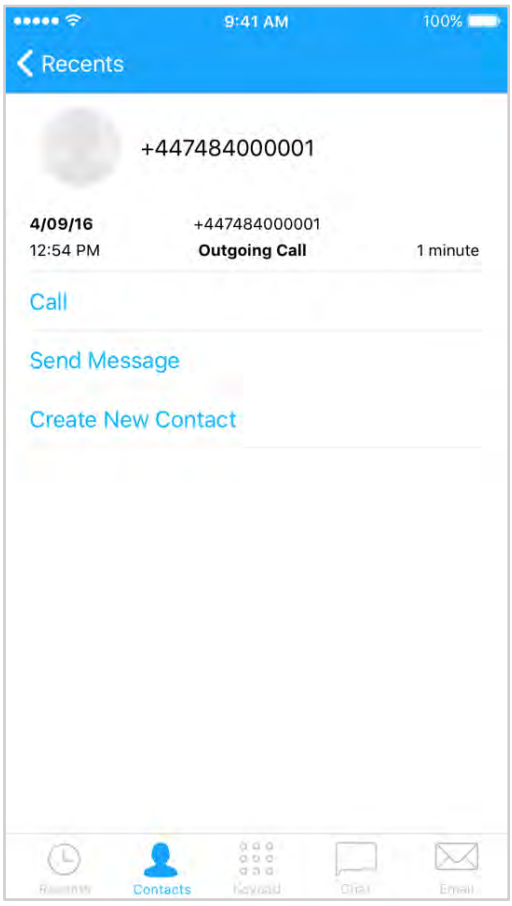




Using the Recents Section

All your previous calls made on your Pryvate app will be listed by tapping the recents button. You can clear the list whenever you wish to. By clicking the info sign on the right side of each entry you will gain more information about that call. You can make calls and add contacts from the detailed info page.





Q. I am having quality issues, What's wrong?

A. If the quality of your call or video call is poor the most likely issue is your bandwidth on your internet connection. You can check it using Speedtest. www.speedtest.net or download their app. If your connection is below 1Mpbs you will start to encounter quality issues.

Q. I have just installed Pryvate but can't make a call to another number which we know works. What can I do?

A. Restarting your device after initial installation will resolve this issue. We suspect it is to do with the security of your device.

Email User Manual

Pryvate Email Client
Log into Pryvate Email
Composing an Email
Reading an Email

Pryvate Email Client

Our Voice, Video, IM and picture sharing part of the App is RSA 4096 level encryption, this is at least twice as strong as our nearest competitor.

For the email client we have chosen to not implement that level of encryption as it will really slow down the whole process. AES 256 is more than adequate for the email service and is resistant against any "quantum brute force algorithm attack" – one of the most dangerous among decrypting techniques

For more details refer this link http://crypto.stackexchange.com/questions/20/what-are-the-practical-differences-between-256-bit-192-bit-and-128-bit-aes-enc

Pryvate Email Client

All your private encrypted emails shall be delivered in an encrypted format to the Recipients Email Service Providers Servers (as normal with un-encrypted emails), thus all emails along with received Pryvate encrypted emails shall show in the usual manner within the email client service providers usual window. However, here all Pryvate encrypted emails cannot be read.

Once you click on any Pryvate Encrypted email within your usual client the email will open and show a link to your Pryvate email Client viewer, click on this button and (so long as you have registered on your Pryvate app email client on your device) your email will automatically be opened and read within your Pryvate email client!

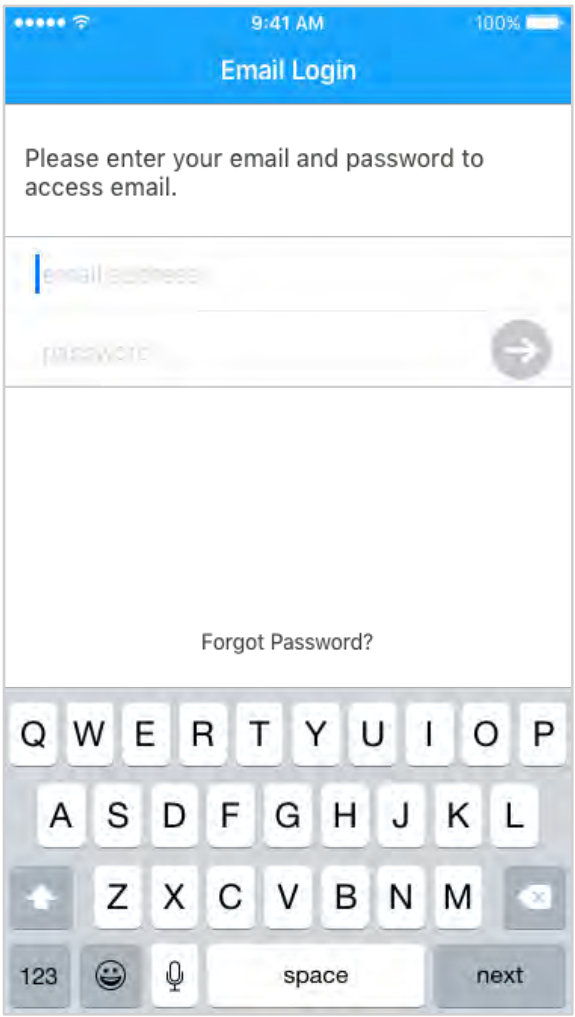
You can read the message, close it, and chose to save the email to your device in its readable format, or you may chose not to save it. If you choose not to save, you can always leave on your current emails server in its encrypted format and access thru the Pryvate client at any time you choose.

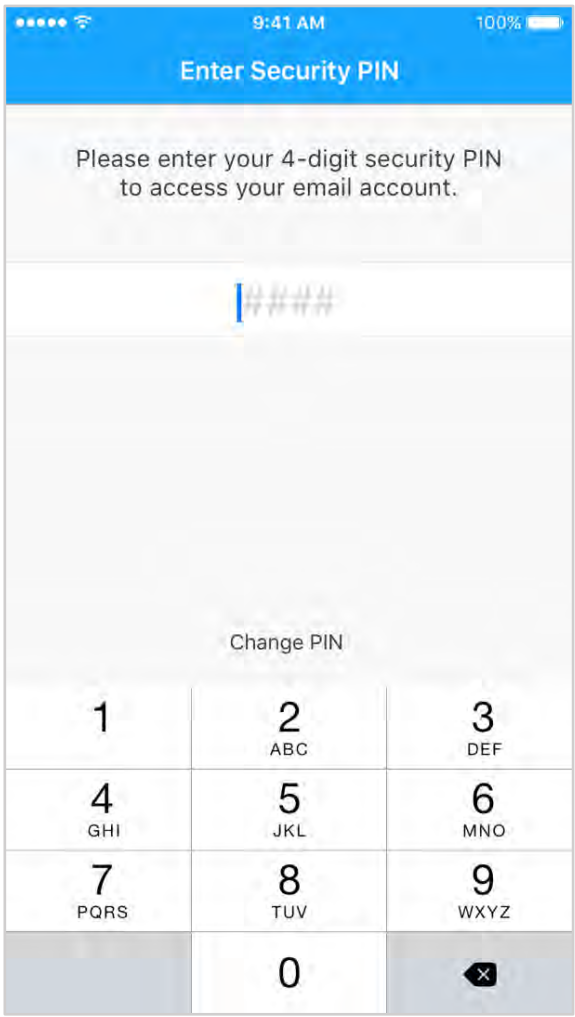
NB. All emails that show on your device are all stored on your email service providers servers, so you can access any of these, whenever sent. These are not stored locally. The same access will be there for your encrypted emails. Nothing changes. Except that all such emails remain confidential and un- readable by anyone other than the intended recipient.

Thus, as we at Pryvate do not store, nor have access to such information, we have provided you with an option for you to store up to 10 emails locally (on your device). We could allow more but realize that this is sensitive information and any more stored locally could start to affect the memory and performance of your service along with leaving decrypted emails viewable on your device!

Log into Pryvate Email

Enter email address you registered with along with password. Your password would have been mailed to your Registered Email Address. If you forgot your password click “Forgot Password” to recover. You will then be prompted for your 4–digit Security PIN.



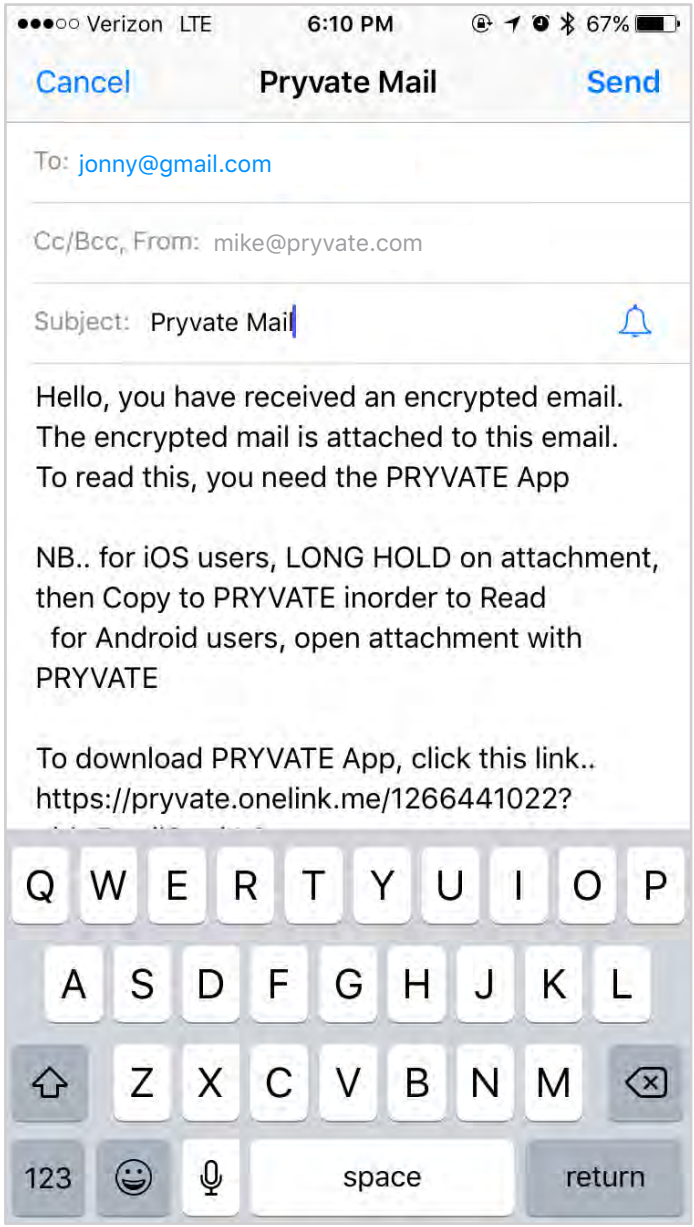


Composing an Email

Once logged in, you can compose and email by pressing the compose icon. Enter the recipients' email address and type your message below. Once you have completed the message, press the airplane button to send.

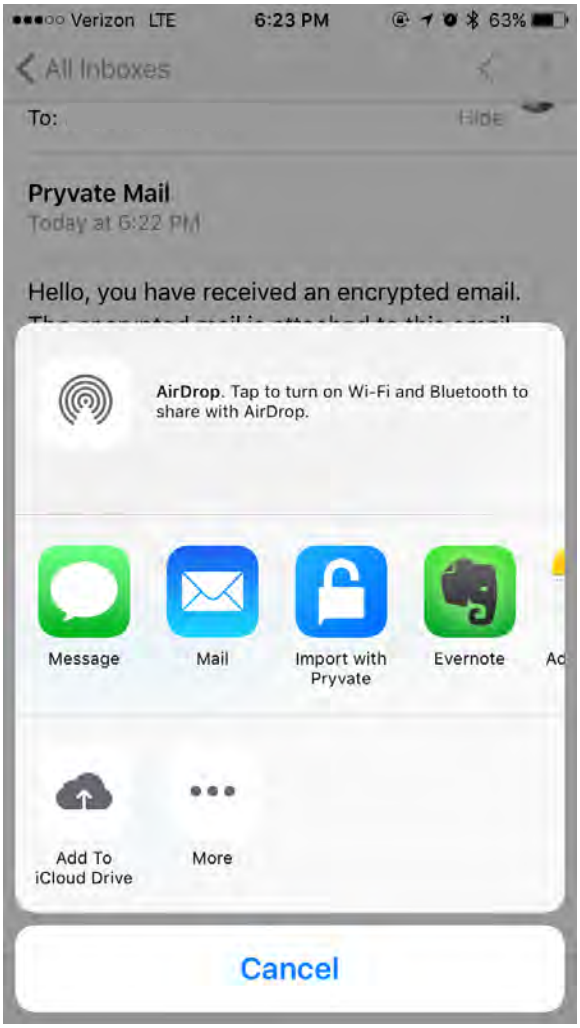
Composing an Email

The sent email will be encrypted and appear in your normal email client as an attachment. You may add a subject line here as usual.



Reading an Email

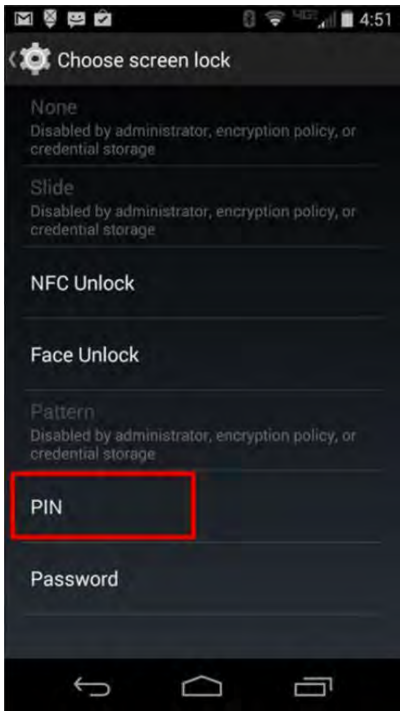
To read an encrypted Pryvate Email, click on the attachment & select “Import with Pryvate” on iOS or “Open with Pryvate” on Android.



Once you have read your message you will be given the option to save your message. If you do not save your message but want to read it again, you can just re-click the link in your normal email client.

Added Security (Android)

To get started, go to Settings > Security > Encryption > Screen lock. Select the PIN option and enter a PIN.



The Android device is ready to be encrypted. Use the settings menu to open the encryption screen below by following Settings > Security > Encryption > Encrypt tablet or Encrypt phone.

Added Security (Android)

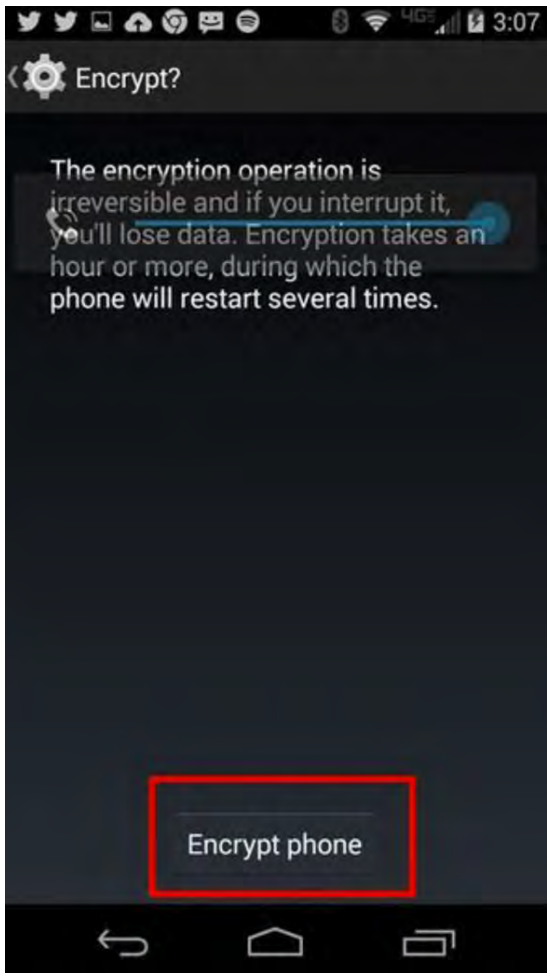
Enter the PIN or password that was created earlier using the screen below. In this case, a short PIN was used to reduce the time to encrypt the device. A longer, random password would be better in practice.

The Android device needs to be plugged in to a charger or it won't encrypt. Tap the encrypt button.
The PIN or Password is required to proceed to the last step to encrypt the device.

Added Security (Android)

Touch the Encrypt phone button. Depending on PIN or password length, encryption can take up to an hour.

The Android device is now encrypted. Every time the Android device is turned on it will require a PIN or password to start.



Added Security (iOS)

Here are some other iOS features you should think about using if you're dealing with private data:

- iTunes has an option to backup your device onto your computer. If you choose the “Encrypt backup” option on the Summary tab of your device in iTunes, iTunes will backup more confidential information (such as WiFi and email passwords), but will encrypt it all before saving it onto your computer. Be sure to keep the password you use here safe.

- If you back up to Apple's iCloud, you should use a long passphrase to protect the data, and keep that passphrase safe. While Apple encrypts most data in its backups, it may be possible for the company to obtain access for law enforcement purposes since Apple also controls the keys used for iCloud encryption.

Added Security (iOS)

- If you turn on data protection as described above, you will also be able to delete your data on your device securely and quickly. In the Touch ID & Passcode settings, you can set your device to wipe all its data after 10 failed attempts.

- According to Apple's old Law Enforcement Guide, "Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running minimum iOS 4. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party App data."

Added Security (iOS)

The above information applies only to iOS devices running versions of iOS prior to 8.0.

- Now, Apple states that “On devices running iOS 8 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key.

- If you are concerned about your device getting lost or stolen, you can also set up your Apple device so that it can be erased remotely, using the “Find My iPhone” feature. Note that this will allow Apple to remotely request the location of your device at any time. You should balance the benefit of deleting data if you lose control of your device, with the risk of revealing your own position. (Mobile phones transmit this information to telephone companies as a matter of course; WiFi devices like iPads and the iPod Touch do not.)

Added Security (iOS)

REMEMBER: While Apple will be unable to extract data directly o a phone, if the device is set to sync with iCloud, or backup to a computer, much of the same data will indeed be accessible to law enforcement. Under most circumstances, iOS encryption is only effective when a device has been fully powered down (or freshly-rebooted, without being unlocked). Some attackers might be able to take valuable data from your device's memory when it's turned on. (They might even be able to take the data when it has just been turned off). Keep this in mind and, if possible, try to make sure your device is powered o (or rebooted and not unlocked) if you believe it's likely to be seized or stolen.

Powered by Criptyque