SMALL WORLD NEWS'

GUIDE TO SAFELY USING SATPHONES

VERSION 1.0 / MARCH 2012

Small World News' Guide to Safely Using SatPhones - Version 1.0 - March 2012

THE GOALS OF THIS GUIDE

This guide provides a comprehensive look at potential uses for satphones in repressive regimes. It contains the best practices on keeping safe while communicating effectively with the least chance for detection & observation.

HOW THE GUIDE WORKS

If you're reading this guide as a PDF on a computer or digital device, text that has a black box around it is a hyperlink to a website. For example:

http://www.mozilla.com/

You can follow these links to learn more, but be mindful about following them on unsafe networks. Some of these sites may flag you for security violations. Follow them only on safe and trusted networks.

TABLE OF CONTENTS

TABLE OF CONTENTS

OVERVIEW

Satellite phones, also known as satphones, are becoming popular communication tools. In areas with low access to traditional communication tools or where communications have been cut off, activists may need satphones to reach the outside world. Using a satphone presents particular risks.

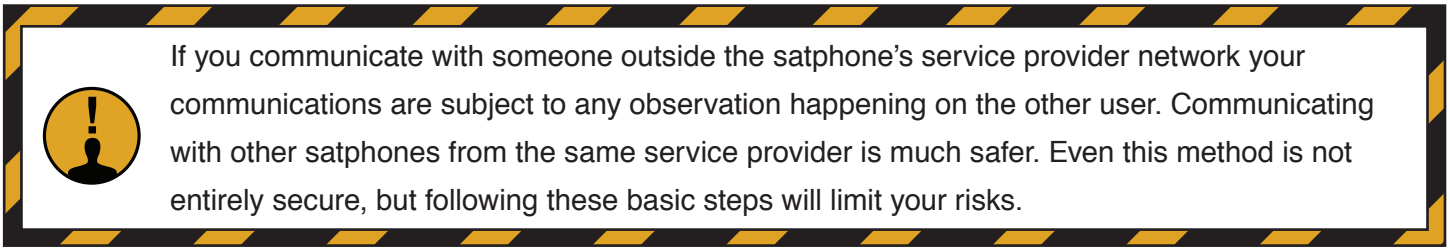
For example, when you depend on this complex technology it is impossible to know exactly how your communication can be monitored. Also, satphones are often banned by repressive governments, and those governments may search for people using them. This guide will assist you to maintain a low profile and improve your chances to evade detection and monitoring from the authorities.

1.0 WHAT IS A SATPHONE?

A **satellite telephone**, **satellite phone**, or **satphone** is a type of mobile phone that connects to orbiting satellites instead of terrestrial cell sites. They provide similar functionality to terrestrial mobile telephones; voice, short messaging service and low-band-width internet access are supported through most systems.

Satphones are complicated radio transmitters. Radios and cell phones use antennas on earth to send out a signal, either a radio broadcast or a phone calls. Satphones send the signal to a satellite in orbit around the earth. The satellite then broadcasts the signal back to earth, to a "Ground Earth Station," or GES. From the GES the signal is sent to the proper communications service provider and to its destination, the receiver of the call. The GES acts as a gateway between your satphone, traditional cellular mobile phone networks, landline networks, and other satphones.

Transmitting information **to** the satellite in orbit is the "uplink." Receiving information **from** the satellite is the "downlink." This information can be data or voice. A phone's signal can be intercepted anytime it has an active connection with the satellite: during the uplink or the downlink.



If you communicate with someone outside the satphone's service provider network your communications are subject to any observation happening on the other user. Communicating with other satphones from the same service provider is much safer. Even this method is not entirely secure, but following these basic steps will limit your risks.

This guide provides the techniques necessary to increase your safety, but is not a guarantee of secure communications.

2.0 OPERATING A SATPHONE

Satphones may look like very large mobile phones, but differ in some key elements. The **Activation** process is relatively similar, while the **Connection** process poses notable differences.

2.1 ACTIVATION

Satphones require activated simcards and must have a plan associated with the simcard. The plan may be prepaid or postpaid. If prepaid the phone must have minutes associated with the simcard. Minutes can be paid for and added online or directly from the phone by submitting scratch card codes via **SMS**.

See **Section 7.2** for details on adding credit to an iSatphonePro satphone.

2.0 OPERATING A SATPHONE

2.2 CONNECTION

Satphones do not connect automatically to their network. Satphones speak directly to one or more satellites in orbit far overhead.

To obtain a signal you must stand still and aim the phone's antenna towards the sky and wait for the phone to locate a signal. Your phone will first obtain a GPS Location fix, then it will connect to the network. This process may take over a minute.

The time needed to connect with the network is the first major security risk.

While you are waiting for the phone to connect you may be observed by the authorities. In **Section 4.2** we will discuss steps you may take to disguise your phone. This can reduce your risk.

NOTE: In order to obtain a signal, the phone must be "deployed" meaning the antenna must be in the on position. Unlike a cellular mobile phone, a satphone will NOT receive calls simply by being turned on. Satphones should not be able to communicate unless the user intentionally connects to the network. This makes it difficult to have unscheduled calls with other satphone users. Therefore, satellite phones should not be depended on for urgent or emergency communications.

2.0 OPERATING A SATPHONE

2.3 USING A SATPHONE, A WALKTHROUGH

This is a complete overview for the steps involved in making a phone call or sending a message from a satphone.

01. Turn on the phone
02. Find a clear view of the sky
03. Engage the antenna to look for a signal
04. The phone obtains a GPS fix.
05. The phone connects to the satellite network
06. Make the call or send an SMS/email
07. The phone uplinks to the satellite
08. The satellite downlinks with a Ground Earth Station (GES)
09. The GES transmits the information to the intended recipient
10. The GES records the phones's GPS locations while transmitting
11. Complete the call or SMS/email
12. The phone logs its GPS Location, the number called, and length of the call
13. Close your antenna
14. Turn off and store the phone

3.0 KNOWN RISKS FROM SAT PHONES

3.1 PHONE CONFISCATION

In many cases, you and your colleagues will be your own worst enemies. There are many technical risks with satellite communication, but the most likely risk is user-generated. These risks are often overlooked because they are primarily caused by normal operation. In repressive states, phone features such as the call log, phone book, and sent folder can endanger your life and the lives of others.

These features help you keep your contacts handy, but they also provide an easily accessed record for the authorities to track your calls, even if they do not have access to your transmissions.

When a file on a computer is deleted, it is not completely destroyed and may be reconstructed without further measures. It is also possible your satphone's logs can be reconstructed from the satphone or data from the service provider.. Deleting information is not a complete fail-safe, but will make it harder for authorities to access information on a confiscated phone.

3.0 KNOWN RISKS FROM SAT PHONES

3.1.1 CALL LOG

By default, your phone will keep a log of everyone you have called. Be sure to delete this every time you make a phone call. Any number you have left in the log will be at risk if your phone is confiscated. It may be suspicious to have an empty call log, but will have less impact on your colleagues.

3.1.2 SENT FOLDER

Similar to the **Call Log**, your phone will maintain a list of **SMS** and **Email** message sent from the phone. Be sure to **Delete** these after every delivery.

3.1.3 PHONEBOOK

Your phonebook is also provides a checklist for the authorities. Any person listed in the phonebook will be at risk if your phone is confiscated. It may be suspicious to have an empty phonebook, but will have less impact on your colleagues.

3.0 KNOWN RISKS FROM SAT PHONES

3.2 SIGNALS INTERCEPTION

All phones are radio transmitters. Satphones send a Radio Signal to a satellite in orbit around the earth. The satellite then broadcasts the signal back to earth, to a “Ground Earth Station,” or GES. From the GES the signal goes through another communications system to its destination, the receiver of the call. A phone’s signal can be intercepted anytime it has an active connection with the satellite: during the uplink or the downlink, when the satellite is sending the receiver’s voice back down to you.

Depending on the equipment available to the authorities, there are different potential risks for signal interception, outlined in this section.

3.0 KNOWN RISKS FROM SAT PHONES

3.2.1 RADIO SIGNALS TRANSMISSIONS

Satellite communications use Radio Signals to transmit information. These transmissions can be triangulated with affordable, even homemade tools. Triangulation uses two or more signal receivers to determine the location of a radio signal transmitter. The location is determined by the receiver based on the axes of the angles of receivers. Highly developed countries with advanced technical security are likely to have this capacity, less developed states and even non-state actors may be able to develop the capacity. For these reasons, keep all transmissions as short as possible.

In some cases the authorities may have the proper equipment to "listen in" on your transmissions, however this requires highly advanced and sophisticated technology. Review section **4.3 Decieve by Speaking in Codes** for tips on how to communicate more safely if you suspect your calls are being monitored.

3.0 KNOWN RISKS FROM SAT PHONES

3.2.2 GPS LOCATION TRANSMISSIONS

Satellite communications require a **GPS Location** for optimal functionality. GPS means Global Positioning System. Your GPS location gives exact coordinates for authorities to find your location. This provides the potential for an individual using any satellite device to be located with exact coordinates. Your location may be logged at the service provider's Ground Earth Station (GES). The GES data may be accessible to many different groups including local or nearby governments, shareholders, local service partners and anyone who is able to hack the GES security systems.

If the authorities possess the correct technology, or have the specific encryption and transmission codes of your satphone brand they may use your phone's GPS coordinates to locate and detain you.

3.0 KNOWN RISKS FROM SAT PHONES

3.3 ENCRYPTION DECODING

Satellite transmissions are encrypted, but many governments are capable of defeating the encryption used by these phones. Standard encryption may deter detection and monitoring but cannot guarantee security.

Thuraya's encryption has been broken, and more advanced governments may be able to break the encryption of other satphones. To learn more see Section 6.2.2

3.0 KNOWN RISKS FROM SAT PHONES

3.3 ENCRYPTION DECODING (CONTINUED)

Satellite communications are vulnerable to prying ears and eyes, who may review voice, message, and data transmissions. Even if the necessary equipment and capability to break the encryption may not be available to the authorities in your area they may be able to break it over time. If the authorities can intercept your Transmissions, and they are capable of recording the signals, it is likely they will eventually break the signal's encryption and review the content of your calls or messages.

In February 2012, two German researchers demonstrated the capability to decode the GMR-1 and GMR-2 encryption standards. These standards are not used by all satphones, but Thuraya and the Inmarsat iSatphonePro both use this standard. The method is fairly technical, however the potential is documented and it is likely that governments will soon begin obtaining the necessary technology.

Given the potential for authorities to obtain such equipment, you should **NEVER** share personal, life threatening, or other critical information via satellite. If you must, please remember to **Speak in Codes** to deter the authorities from understanding.

4.0 PRECAUTIONS FOR LIMITING RISK

Satphones are closed technology, and not easy to modify. Because of this it is impossible to have completely secure communications with a satphone. However, these basic precautions can be used with any satphone to increase your safety and decrease the risk of observation or detention by authorities.

4.1 DELETE ALL RECORDS

Do not save communications information on the satphone. Although security services may obtain calling records through other means, do not make it easy for them. Even without names a list of phone numbers, cellular or satellite, for authorities to track and locate could be catastrophic. Each phone manufacturer has a different system, so become familiar with the steps to delete records on your phone as soon as possible.

See **Section 7.0** for specific steps to make the Inmarsat iSatphonePro safer.

When communicating with individuals who may be threatened or under surveillance, be sure to maintain their information in a safe and secure location.

4.0 PRECAUTIONS FOR LIMITING RISK

4.2 DISGUISE YOUR PHONE

When using the phone for calls, do not leave it out in the open. Always pair with a headset, so it will appear you are using the local cellular network not making a satellite call. Using a Bluetooth headset will make it easier to disguise the phone, however there are additional security risks, listed in section 7.5.

Keep the phone hidden at all times and disguise it if you have time. Place the phone in a location with a good angle toward the satellite's position, but disguise its physical location as much as possible. Put the phone inside an open bag, or behind some bushes. This may be difficult as the phone needs a clear view of the sky. If possible experiment in a safe location to see how you can evade observation without interfering with the phone's connection.

4.0 PRECAUTIONS FOR LIMITING RISK

4.3 DECEIVE BY SPEAKING IN CODE

In cases where you are communicating with collaborators, fellow activists, etc. hide your true intentions. Use codes, discuss common subjects that you are likely to share, yet have double meanings. Do not discuss your intentions directly.

EXAMPLE:

Use memorable phrases and terms with double meanings, or use familiar subject matter such as specific religious verses. For example, use a term to indicate authorities such as “uncle.”

When checking with a contact to first determine whether the contact is safe from authorities, one might ask, “Has your uncle come to town?” Yes may indicate it is not a good time to talk, no indicates it is safe.

This enables further codes, your contact could say “My uncle was here, but he left, I’m going to be busy for the next few days,” indicating it’s inadvisable for you to try and reach your contact in the near future.

Additionally “My Uncle was here, he reminded me that the family reunion is happening soon,” could indicate the authorities may be planning to interrogate you or your other colleagues soon.

4.0 PRECAUTIONS FOR LIMITING RISK

4.3 DECEIVE BY SPEAKING IN CODE (CONTINUED)

You may also want to consider codes that are don't have such a direct relationship, where the combination of subjects discussed provides information. Also providing false or misleading information, such as a location, can confuse anyone who may be listening in.

For example "Did I tell you about my cousin's wedding that is coming up? She is marrying a very good man from Aleppo." In this case the term "wedding" and "very good man" could be operative phrases, where wedding indicates the authorities may be looking for you soon, and "very good man" indicates the specific security service involved. Using another phrase such as "wealthy merchant" will indicate a different office.

Covering your intentions may save your life or others.

4.0 PRECAUTIONS FOR LIMITING RISK

4.4 DESTROY YOUR SIMCARD AND PHONE

If your phone is confiscated, the simcard will provide information that can be used against you and your colleagues. Keep the simcard out of the phone so it can be quickly destroyed. If possible destroying your phone may further limit your risk, however its more important to follow the previous 3 precautions and attempt to avoid detection by the authorities.

5.0 USING YOUR SATPHONE MORE SAFELY

The previous section outlined basic precautions you can take with any satphone. This section explains specific techniques for using your satphone more safely in each of the primary uses, making voice calls and sending SMS or email messages.

5.1 VOICE CALLS

Voice calls are a very risky method for communicating via satellite. When making a call, be sure to keep the call as short as possible, due to the potential for interception of your phone's **Radio Signals**, or **GPS Location**.

Authorities may use your phone's **Radio Signals** to detect your position within less than three minutes. As their techniques become more sophisticated they may be able to locate a satphone even more quickly. In some cases authorities may be able to listen in to your phone call, by intercepting its **Radio Signals** transmissions. Authorities may tap the phone at the other end, if they have access to service provider.

The longer you remain on the line, the greater opportunity you provide the authorities to find your exact position via your phone's **GPS Location**.

5.0 USING YOUR SATPHONE MORE SAFELY

5.1 VOICE CALLS (CONTINUED)

When making an interview, be sure the interviewer is clear on your situation and do not remain on the line longer than you feel safe. It is best to keep your call under three minutes. Prepare your comments beforehand, and be clear that you will not discuss items outside your planned communication.

When making a Voice call to communicate with a colleague or coordinate with other activists, remember to **Speak in Codes**. This is important in order to **Deceive** anyone who may be listening in, or may break your phone's **Encryption**.

Speaking in Codes and using common phrases that have a double meaning may keep you or others safe, though you may not know your conversations are being monitored. Utilize common phrases, rather than special words you would not otherwise discuss.

Delete your phone's call log. There is nothing worse than creating an indexed archive of information that is waiting for the authorities. If you fail to do this, you will put others at risk and may increase the potential threat to yourself if your phone is confiscated.

5.2 SMS

SMS is a highly convenient method of sending a message. When sending an SMS from a satphone that message is delivered via email, where your phone number is attached to a carrier specific server address, such as 5555555@text.phonecarrier.com.

Despite manufacturer claims, SMS does not provide secure encryption. Do not transmit sensitive information via SMS unless you are willing to have it read by the authorities. If the SMS is intercepted, it is likely to be recorded and the **Encryption** broken at a later date, if not immediately.

SMS may take less time than a voice call, so the risk of intercepting the SMS Radio Signal or exploiting the phone's **GPS Location** may be less than with voice. However it is more likely the content of your message will be retrievable by the authorities, if your **Transmission** is intercepted.

Deceive unwanted observers through the use of code phrases and terms with double meaning. **Delete** SMS from your phone's sent folder. There is nothing worse than creating an indexed archive of information that is waiting for the authorities to review in the event you are detained.

5.3 EMAIL

Email can be sent via any satellite phone, but is delivered via the same protocols as SMS, and restricted to approximately 160 characters.

You may decide to use the email feature rather than SMS because you expect email to be more secure. This is incorrect. Email sent from your satphone does not provide the same protection as Email sent via computer or mobile data plans.

Computer and mobile internet both provide the opportunity to use additional security tools. Email can be sent by computer or mobile over an **HTTPS** connection that is far more difficult to intercept. On some mobile phones and all computers **Tor** can be used to anonymize your computers traffic and hide your identity and location. If at all possible use a secure internet connection to communicate, not a satphone.

5.3 E-MAIL (CONTINUED)

Because, like SMS, an Email transmission may take less time than a voice call, risk of intercepting the message via the Radio Signal or exploiting the phone's GPS Location may be less than with voice. However it is more likely the content of your message will be retrievable by the authorities, if your Transmission is intercepted.

Deceive unwanted observers through the use of code phrases and terms with double meaning. Delete Email from your phone's sent folder. There is nothing worse than creating an indexed archive of information that is waiting for the authorities to review in the event you are detained.

6.0 CHOOSING WHAT BRAND TO USE

All satphones are not equal. Each brand has its limitations, though as will be explained, we recommend not using Thuraya phones if you can avoid them. That warning aside, the previous sections will still provide the best practices to follow to limit your risk.

There are a variety of satellite communications service providers, including Thuraya, Inmarsat, Iridium, and GlobalStar. Others such as MSV, ICO, Teledesic are currently non-operational or do not provide consumer services.

Based on our research, although no satphone is truly safe and secure from determined authorities, we have found that Thuraya, in particular, is unsafe, and should be avoided at all cost. We are recommending Inmarsat's iSatphonePro for ease of use, availability, and its recent rise as an entry-level device used by many journalists and activists across the Middle East.

6.0 CHOOSING WHAT BRAND TO USE

All satphones are not equal. Each brand has its limitations, though as will be explained, we recommend not using Thuraya phones if you can avoid them. That warning aside, the previous sections will still provide the best practices to follow to limit your risk.

There are a variety of satellite communications service providers, including Thuraya, Inmarsat, Iridium, and GlobalStar. Others such as MSV, ICO, Teledesic are currently non-operational or do not provide consumer services.

Based on our research, although no satphone is truly safe and secure from determined authorities, we have found that Thuraya, in particular, is unsafe, and should be avoided at all cost. We are recommending Inmarsat's iSatphonePro for ease of use, availability, and its recent rise as an entry-level device used by many journalists and activists across the Middle East.

6.0 CHOOSING WHAT BRAND TO USE

6.1 WHY NOT THURAYA?

6.1.1 BACKGROUND

Thuraya became one of the more popular satellite communications companies, due to its affordable products and broad functionality, particularly in the Middle East. Throughout 2011 the popularity of Thuraya began to decrease, due to the ease with which governments are able to block or intercept Thuraya. Blocking was first seen over 6 months in 2006 as the Libyan government engaged in massive jamming of the service from within its territory. Likely due to Thuraya's popularity in the Middle East the United States targeted this provider in particular for interception and encryption decoding.

6.2.2 THURAYA'S PROBLEMS

In 2011 Syrian activists alleged the Syrian government compromised Thuraya's network security. It is believed that Rami Makhlouf controls the Syrian subsidiary of Thuraya. Activists believe he obtained access to Thuraya's decryption codes and other records and provided these to the Syrian regime. Detained activists have later reported hearing recordings of conversations they made over satphones. We have been unable to determine if the recording happened by interception of an uplink. It seems likely the activists was communicating with someone on a local service provider that was tapped by the authorities.

In 2011 Syrian activists alleged the Syrian government compromised Thuraya's network security. It is believed that Rami Makhlouf

6.0 CHOOSING WHAT BRAND TO USE

6.2.2 THURAYA'S PROBLEMS (CONTINUED)

controls the Syrian subsidiary of Thuraya. Activists believe he obtained access to Thuraya's decryption codes and other records and provided these to the Syrian regime. Detained activists have later reported hearing recordings of conversations they made over satphones. We have been unable to determine if the recording happened by interception of an uplink. It seems likely the activists were communicating with someone on a local service provider that was tapped by the authorities.

According to Strategy Page, in 2003, "Thuraya recently announced that while the phones did transmit the GPS location periodically (to insure a good signal), the information was sent in encrypted form and only someone with access to the codes, or with powerful decryption capabilities, could get the location information (of the phone broadcasting the information)."

It is also documented that the US, and possibly Indian authorities were able to listen in on conversations between individuals using Thuraya phones, ahead of the terrorist attacks across Mumbai in 2008, "Officials say one of the phones recovered was a Thuraya satellite phone. "Once we have the number we will be able to know everyone who was called and where the calls were made from," one former intelligence office says."

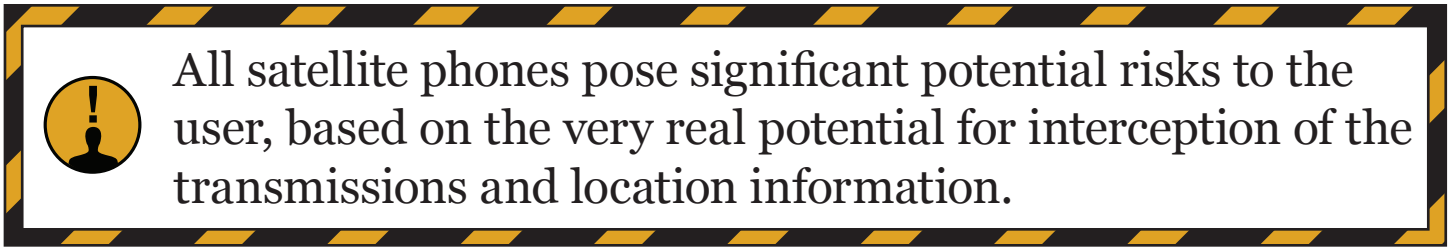
Based on this information, we recommend activists avoid using Thuraya phones in any circumstance.

6.0 CHOOSING WHAT BRAND TO USE

6.2 WHY USE INMARSAT'S ISATPHONEPRO?

Why do we believe the iSatphonePro is safer than Thuraya, and relatively as safe as other brands? While Thuraya is definitely compromised, other services may be compromised as well. The contents of this guide will assist you to maintain the greatest amount of safety possible, despite the serious risks posed by satellite communications technology.

At the time of publication, January 2012, there were no known exploits of Inmarsat phones by the Syrian authorities. As a company based in the United Kingdom, there are legal constraints preventing Inmarsat from providing records to the Syrian Government. At the time of publication there were no accounts of Inmarsat phone users detained due to the operation of an Inmarsat phone.



7.0 HOW TO IMPROVE THE SAFETY OF AN ISATPHONEPRO

In many cases, you and your colleagues will be your own worst enemies. Although there are many technical risks with satellite communication, the most likely risk is user-generated. These risks are often overlooked because they are primarily caused by normal user operation.

In the case of repressive states, phone features such as the call log, phone book, and sent folder can endanger your life and the lives of others. These features keep your contacts handy, but also provide a record for the authorities to track your calls, even if they do not have access to your transmissions.

These directions will make the iSatphonePro safer and help you avoid the risks mentioned in this guide.

7.0 HOW TO IMPROVE THE SAFETY OF AN ISATPHONEPRO

7.1 LOCK YOUR PHONE

To prevent unwanted eyes from examining your phone, turn on the admin code, and pin request functions. This may be found by accessing:

Menu > Settings > Security

When choosing number codes **DO NOT** choose codes with all the same number, or easy combinations such as 1111 or 1122. By default the admin code is 123456, this code must be 6 digits. If you mis-dial your code you can reenter an unlimited number of times.

The SIM pin by default is 8888, this code must be between 4 and 8 digits. The SIM pin 2 by default is 9999, this code must be between 4 and 8 digits. If the SIM codes are entered incorrectly three times your SIM will only be unlocked by obtaining the PUK code.

7.2 ADD PHONE CREDIT REMOTELY

To add credit to your iSatphonePro you need to first purchase credit. This can be done at a number of websites, such as: http://satphonecity.com

To check your phone's balance, make a call to this code: ***106#**

To add balance to your phone from a voucher, enter the following code: *101*VoucherNumber#

For example: *101*123456789#

7.3 CLEAR YOUR CALL LOG

By default, your phone will keep a log of everyone you have called. Be sure to delete this every time you make a phone call. Any number you have left in the log will be at risk if the phone is confiscated. It may be suspicious to have an empty call log, but will have less impact on your colleagues.

Delete the Call Log by accessing:

Menu > Call Log > Options > Clear all

7.4 DELETE YOUR SENT FOLDER

Similar to the Call Log, your phone will maintain a list of SMS and Email message sent from the phone. Be sure to Delete these after every delivery.

Delete SMS and Email messages by accessing:

Menu > Messaging > Sent > Options > Delete all messages

7.5 DELETE YOUR PHONEBOOK

Your **Phonebook** also provides the authorities a checklist if it list your colleagues' phone numbers. Any number left in the phonebook will be at risk if the phone is confiscated. It may be suspicious to have an empty phonebook, but it will have less impact on your colleagues.

Delete your Phonebook by accessing:

Menu > Contacts > Phonebook > Delete all

You can delete any contacts stored on the simcard by accessing:

Menu > Contacts > Sim Contacts

7.6 USE A BLUETOOTH HEADSET TO MINIMIZE SUSPICION

Do not leave the phone out in the open. Keep it hidden at all times and consider disguising the phone.

When using the phone for calls, if at all possible, pair with a headset. It will appear you are using the local cellular network, not making a satellite call. Place the phone in a location with a good angle toward the satellite, but disguise the phone's physical location. Using a bluetooth headset will make it easier to disguise the phone, but may result in other risks listed below.

Activate the phones' bluetooth capacity by accessing:

Menu > Settings > Bluetooth > Paired Devices > Options > Search for devices

7.0 HOW TO IMPROVE THE SAFETY OF AN ISATPHONEPRO

7.6 USE A BLUETOOTH HEADSET TO MINIMIZE SUSPICION (CONTINUED)

NOTE: When "discoverable" your Bluetooth signal will be visible to devices detecting Bluetooth transmissions within 10 meters. Always keep your Bluetooth non-discoverable. NEVER connect your satphone to an unknown Bluetooth device. Always use a headset with a "push-to-sync" button. The Bluetooth signal switches randomly among 79 radio frequencies, 1600 times per second, making it very difficult to intercept the transmission.

There is equipment on the market that will enable anyone to monitor, record, and decrypt Bluetooth audio transmissions in real time. The likelihood of authorities to have access to this equipment is unknown, though not impossible. If you are not currently being monitored, it will be difficult for the authorities to observe you, based on your Bluetooth transmissions alone. If the authorities do locate you, it is feasible they can obtain a receiver capable of picking up Bluetooth transmissions from more than a kilometer away.

7.7 DISABLE YOUR PHONE AND KEEP YOUR SIMCARD SECURE

The satphone will not connect with the network, and should not transmit GPS or other signals when the antenna is not deployed. Remove the simcard and keep it with you, this will make it easy to destroy in the event of confiscation. Always close the antenna to **disable** the phone when not in use.

In the case of the iSatphonePro a large coin works well.