

# SAE SYSTEMS

## SafeTalk (STP)

The SafeTalk (STP) mobile phone pouch is designed to prevent unauthorised activation and monitoring of your cellular phone that can lead to disclosure of your private or business information.



STP is a modified mobile phone pouch with an embedded electronic module that constantly monitors phone's electromagnetic emission. If your phone, while in a pouch, suddenly starts voice transmission, STP instantly turns on the audio noise generator thereby masking any nearby conversation.

STP controls all GSM, CDMA-2000, UMTS, BLUETOOTH and WLAN (2,4GHz) frequencies.

SafeTalk (STP) (above) has an appearance of an ordinary leather type pouch suited for the majority of mobile phones including Blackberry and iPhone. In reality, this innocent looking case is the most advanced means of safeguarding phone privacy. STP prevents secret recording and transmission of conversations via switched on mobile without the owner's knowledge or authorisation. To keep your privacy put a mobile phone into a pouch and switch the latter on. From then on no secret recording or voice transmission via your mobile will be possible.

FT.com (Financial Times) August 2, 2005.

If ordered to do so, mobile telephone operators can also tap any calls, but more significantly they can also remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call, giving security services the perfect bugging device. "We have inadvertently started carrying our own trackable ID card in the form of the mobile phone," said Sandra Bell, head of the homeland security department at the Royal United Services Institute. (To read full article visit:

[http://www.ft.com/cms/s/0/4239e29e-02f2-11da-84e5-00000e2511c8.html?nclick\\_check=1](http://www.ft.com/cms/s/0/4239e29e-02f2-11da-84e5-00000e2511c8.html?nclick_check=1) )

BBC News. 2 March, 2004

News that Kofi Annan and other senior UN figures may have been routinely bugged by US or British security services has caused a huge political row around the world. But it will also have caused alarm among other people in the public eye who deal with sensitive information - or anyone, indeed, who values their privacy.

Today's spies are able to convert conventional phones into bugs without the owners' knowledge.

Experts believe this is the most likely method used to gather information in the UN building.

So provided it is switched on, a mobile sitting on the desk of a politician or businessman can act as a powerful, undetectable bug <http://news.bbc.co.uk/1/hi/magazine/3522137.stm> )

'FBI Activates Cell Phones Remotely for Wiretapping' – December 2, 2006

It has been recently revealed that the U.S. Federal Bureau of Investigation has a way of tapping a cell phone and using the microphone to listen in on nearby conversations.

The method used for listening in on conversations held by alleged members of Cosa Nostra is called a "roving bug" and was ruled to be a legal method of wiretapping by U.S. District Judge Lewis Kaplan. It looks like all cellular phones are vulnerable to this sort of wiretapping according to CNet's findings:

The U.S. Commerce Department's security office warns that "a cellular telephone can be turned into a microphone and transmitter for the purpose of listening to conversations in the vicinity of the phone." An article in the Financial Times last year said mobile providers can "remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call."

<http://www.dailytech.com/FBI+Activates+Cell+Phones+Remotely+for+Wiretapping/article5184.htm>



**Voice Interception:**

Means of remote mobile phone interceptions:

1. Any cellular network provider can switch a phone into 'police mode' without your knowledge.
2. Your cellular phone may have been modified to enable a 'third party' to listen in on your conversations by calling your cellular using a special preprogrammed number.
3. The mobile may be infiltrated with a virus or special program capable of sending speech information through GSM, BLUETOOTH or WLAN (Wi-Fi) channels.

**Usage:**

ACTIVATION- Press and hold the STP's side ON/Off button for 3 seconds. The LED turns on and a sound is played.

DEACTIVATION- Press and hold the side button for 3 seconds. The LED turns off and a sound is played.

WORKING MODES AND INDICATION-In Radio Watch Mode the LED flashes at the rate of about 1 per 2.5 seconds, which is also a radio monitoring rate. If a short press of a button is confirmed by a short beep - RW Mode is on. If the STP detects a voice transmission, it switches into Audio Noise Mode and the audio noise generator turns on and LED starts blinking frequently. If the voice transmission is stopped, STP switches back into Radio Watch Mode. In Sleep Mode the LED does not blink. If a button is short pressed, there will be no beep sound. Power consumption in Sleep Mode is so low that the STP battery may not be changed for several years.

BATTERY CONTROL-If a battery level drops below 2.2V, LED changes its color from green to red. In Audio Noise Mode signal 'Battery Low' is played every minute.

**TECHNICAL DATA**

Characteristics	Units	Min	Type	Max
Supply Voltage	V	2,0	-	3,3
Supply Current in Sleep Mode	µA	-	2,4	4,0
Supply Current in Radio Watch Mode	µA	-	100	120
Supply Current in Audio Noise Mode	mA	-	9,0	13,0
Frequency Band	MHz	300	-	3000
Operating temperature	°C	-20	-	+50
Working Time in Radio Watch Mode CR2032	Days	-	90	-
Working Time in Radio Watch Mode CR1632	Days	-	50	-

**WORKING CONDITIONS**

The STP may be used in wide temperature range: from -20°C to +50°C, as well as in rain or snow of moderate intensity. If the STP is used in damp or wet conditions it should be dried out after use. The STP is not suitable for submersion.

**CHECKING WORKING MODE WITHOUT LED**

To preserve the customer's anonymity some STPs can be supplied without an LED light, only with a sound button.

**STP SIZE TABLE**

To determine which pouch fits your phone and which type of fastener you want please refer to the table below:

Internal Dimensions LxWxD, mm	Name	Reference
98x53x21	"Supercase", artificial black leather, universal fastener (clip and belt loop)	SC001
104x53x21	"Supercase", artificial black leather, universal fastener (clip and belt loop)	SC002
98x46x15	"Supercase slim", artificial black leather, universal fastener (clip and belt loop)	SC003
98x44x15	"Nobby type 7 slim", natural leather black buffalo, clip	N12219



102x46x21	"Nobby type 7", natural leather black buffalo, belt loop	N2652
102x46x21	"Nobby type 7", natural leather black buffalo, clip	N2655
115x50x23	"Nobby type 8", natural leather black buffalo, belt loop	N2653
110x50x23	"Nobby type 8", natural leather black buffalo, belt loop	N2653Y
117x52x23	"Nobby type 8", natural leather black buffalo, clip	N2656
110x52x23	"Nobby type 8", natural leather black buffalo, clip	N2656Y
106x68x22	"Nobby type L", natural leather black buffalo, clip	N12222
117x70x21	"Nobby type XL", natural leather black buffalo, clip	N12223 (Blackberry +iPhone)

## SUMMARY

There are two ways to retain your mobile phone privacy.

1. Take out a battery and disable the phone completely. Having done so, you lose connection with the world and control of the situation.
2. Put a mobile into a SafeTalk Pouch and switch it on. Stay in total control of the situation and in touch with people you need.