Stealth Phones

The meaning of security.

"Which mobile phone will help me protect myself from various attacks?" To answer this question, it is important to know who you need to protect yourself from. Are you looking for protection from prying eyes like a business partner, from hackers, or from professional institutions such as spy companies, unscrupulous corporations or abusive governments? Evaluating the answer and analysing the various "secure mobile phones" takes a lot of time and needs to be done by experienced experts.

Vendors and developers of "secure mobile phones" take advantage of end-user's lack of understanding of this complex issue by suggesting security without mentioning what their protection applies to. **End users run the risk of using a "secure phone" that does not meet the necessary requirements.**

Interception of telecommunications is becoming an increasing problem.

"What is the intention behind the interception of individual telecommunications?" Interception and surveillance of citizens is an extremely serious matter. The ability to invade privacy is an enormous power that can be used to monitor, embarrass, control, shame or even ruin a person. Our right to privacy protects us from being persecuted for our beliefs, our religion or our lifestyle.

Because the technology of interception is so crucial, it has been subject to carefully crafted and legal controls almost since its invention. Ignoring these controls and intercepting without a warrant is a criminal offence punishable by significant prison sentences in any country. Yet all this is ignored and warrantless interception of citizens has become a daily routine even in democratic countries.

The distinction between legal and illegal surveillance is no longer possible, as more and more private companies have access to surveillance and interception systems, and even a moment of corruption is enough to use the information obtained to their own advantage. Our privacy is under attack without us being aware of it.

> A "secure cell phone" must protect cell phones users in all circumstances, treat all threats equally, and not distinguish between legal and illegal interception.

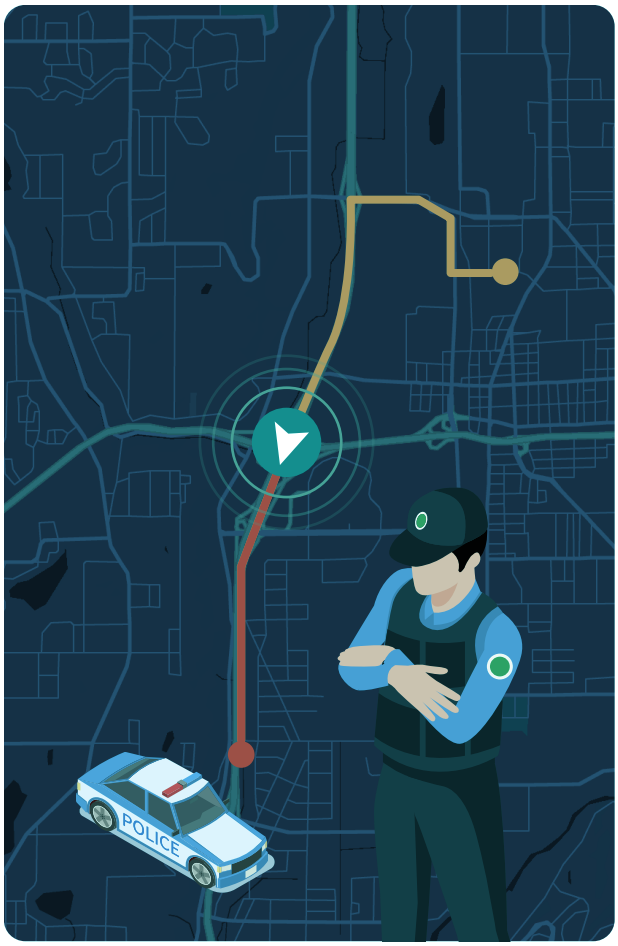
"There is no technological difference between legal and illegal interception" Legal interception must be authorised by an official in order for the results to be admissible in court. Illegal measures use the same surveillance and interception technologies, but without authorisation or control by a higher authority because the results are not collected for official use in court. **Illegally obtained results serve as a basis for authorising legal surveillance, whose newly obtained results are valid in court.**

"The identity of the target matches the identity of the mobile phone" Any mobile phone is actually a tracking device that can be used to make calls, send messages and use the Internet. A mobile phone identifies itself to the network with two 15-digit serial numbers, which can be used to uniquely identify a mobile phone anywhere in the world.

The IMEI
Unique phone registration number.

The IMSI
Unique SIM registration number.

As soon as the phone is switched on, **it automatically connects to the strongest signal cell tower,** even without a SIM card inserted! No matter the make, OS, price or technology (2G, 3G, 4G or 5G). This process repeats periodically. This prevents the phone from accidentally disconnecting from the network. However, this basic function of establishing a connection also serves another purpose: locating a target phone. The establishment of a connection can be abused by private and state entities to determine the location of the phone user at any given time. Mobile operators store every connection based on the identity of the mobile phone and the identity of the tower. These records can be subsequently requested by the authorities or can be downloaded directly from the cell tower when needed, as they do in the US (called tower dump procedures). Since this process is repeated regularly, the location of cell towers can be used to create an almost complete profile of a user's movements.



Only call data such as date, time, duration, direction, phone numbers, IMEI's and IMSI's involved, location of all cell phones involved in conversation are recorded retrospectively. It is not possible to analyse voice call content, SMS text content and data content in retrospect without a warrant issued before. The content of the communication is evaluated in real time or, if there is an active interception warrant, will be analysed during the monitoring process (1 day to 6 months). This can be done at the direct level of the mobile core network by exploiting known SS7 vulnerabilities, or with the help of mobile surveillance and interception systems explicitly designed for telecommunications interception.

> A "secure phone" must be able to change its identity by changing its IMEI and IMSI, and must have features to detect interception attempts. Relying only on a phone's encryption alone is no guarantee for security against professional interception methods, aka lawful interception.

Cell phones that rely only on encryption have no protection against call/SMS interception, monitoring and location tracking performed by hackers using lab equipment such as a moded femtocell, SDR devices, site simulators, network testing devices, and USRP type devices. Unskilled hackers can only sniff the air interface, gathering off the air some data as IMEI's, IMSI's, phone numbers, relative location and – sometimes – SMS text content – but cannot actually intercept a phone call. Skilled hackers with proper hardware can do the same as law enforcement do: intercept phone calls, SMSs, data traffic (including account credentials, chat content, messenger content, etc.) and location tracking up to +/-3 meters accuracy.

A crypto phone is not as secure as you think. A mobile operator or the institution operating a GSM interceptor can find out important information such as contacts, exact location and communication behaviour of the user. This information can (and will) be used to discover your secrets which will be valued as legal proofs against you, in front of a Court.

Interception detection as a security advantage

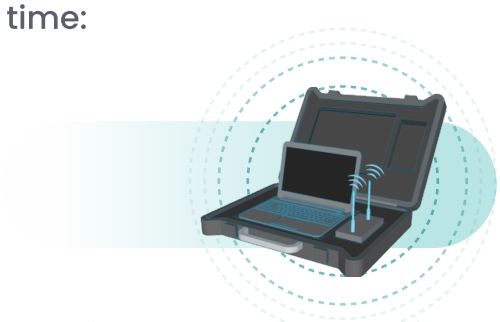
We often equate mobile security with physical security. A company hires a security guard and posts him at the front door of the building. The guard stands at his post. He checks IDs and provides security at the entrance. Because he is at the front door, he cannot monitor all areas of the company. If someone simply jumps the fence and enters, he cannot see that there is a security risk.
The same applies to the use of an encryption solution (software or hardware): You will never know when your mobile phone is being tapped. **So you will never know when you are at risk.**

Not to mention that anyone (even a kid or average Joe) that have a simple and cheap radio jammer can remotely disable any sophisticated secure cell phone, by jamming downlink channel or, as law enforcement do, jamming only data channel. This will certainly force the phone user to use its phone as a regular cell phone, making and receiving regular phone calls and send/receive regular SMSs, which are in these circumstances easily intercepted.

> A "secure mobile phone" must detect call/SMS interception attempts and alert the user in real time. Only by being alerted in real time is it possible for the user to ensure the safety of his life and to adapt his behaviour to new threats.

Stealth Phones for mobile security, there is no substitute. The rest of the market is going the way of text and voice encryption, which only gives the user a false sense of security. XCell Stealth Phones go straight to the heart of the problem by exploiting the same network vulnerabilities responsible for user identification, location, voice and data interception.

"Interception Detection" Stealth Phones can detect all types of call, SMS and data interception and alert the user in real time:



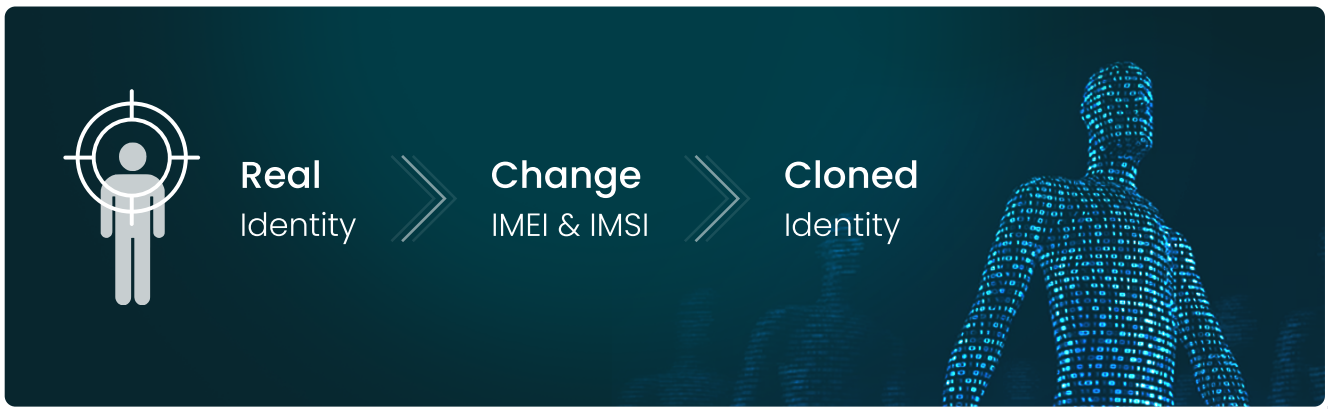
- ✓ IMSI Catchers.
- ✓ Active GSM-Interceptors.
- ✓ Semi Active GSM-Interceptors.
- ✓ Passive GSM-Interceptors.
- ✓ SS7 means (by the help of network provider, called also Lawful Interception).

Stealth Phones will also detect if the other mobile phone that is involved in the call is being tapped.

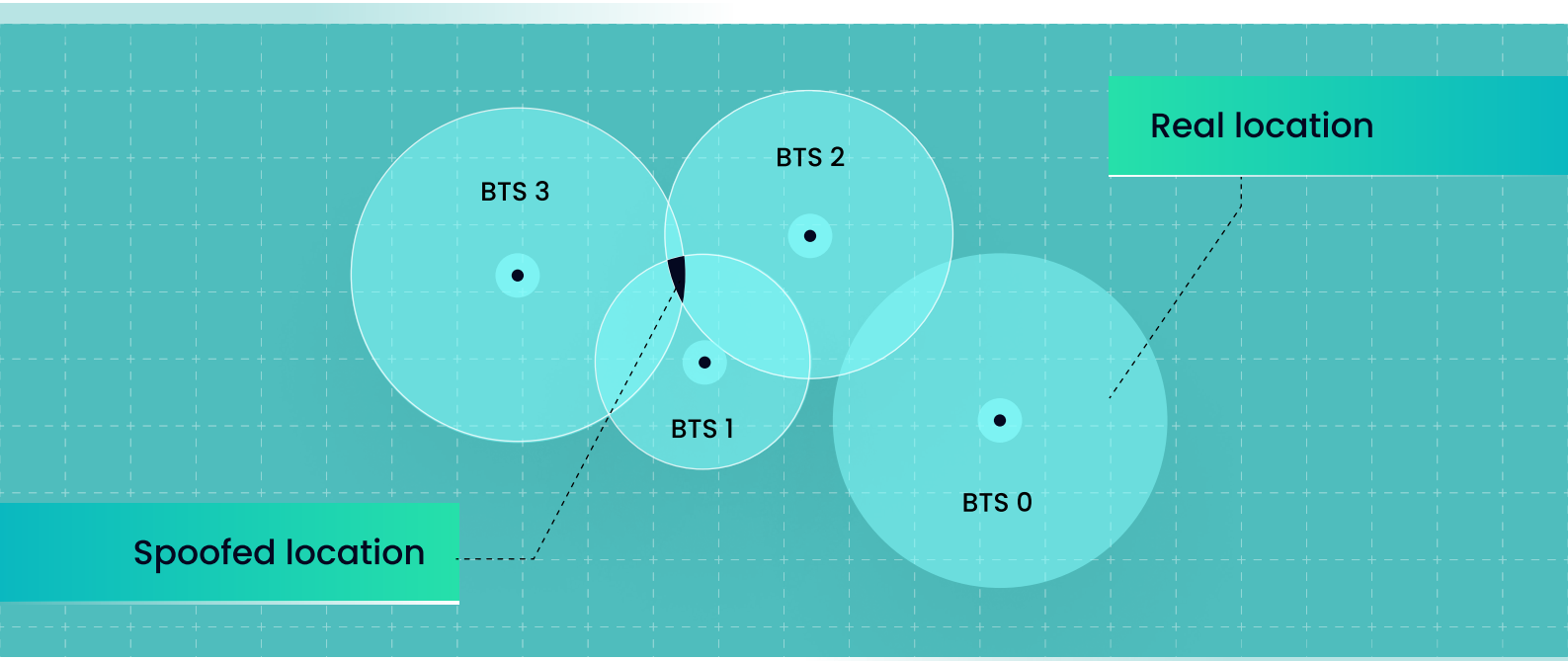
"User Identification" Some Stealth Phones are equipped with an automatic IMEI and IMSI change function that turns your mobile phone into an intelligent counter-intelligence weapon. The simultaneous IMEI and IMSI change prevents location, voice and data surveillance. The fact that all your phone identifiers have been changed (previously registered in the target selection list of a GSM interceptor or mobile operator) means the operator then does not know who needs to be monitored. The interceptor must make extra efforts to obtain and register your new identifiers.

If the IMSI is not changed locally on the phone (as only XCell Stealth Phones do) without using internet connection (and backed by servers that cannot be checked out and trusted by the user) but via the internet connection by the SIM issuer as some Russian and Polish companies do, that will not solve the problem because an IMSI Catcher or GSM Interceptor with jamming capabilities will disable such IMSI change SIM cards at a glance. Actually, this became a common practice nowadays among GSM Interceptors human operators.

Note: If you have only changed the IMSI (SIM card) or only the IMEI, you will not get any added value and your calls will still be intercepted as if you had not changed anything, as a correlation between unchanged and changed IMEI and IMSI value can be detected.



"Location Spoofing" Some Stealth Phones are equipped with a "real location spoofing" feature, which is a real GSM location manipulation based on cell tower manipulation that give out a fake triangulation result. GSM triangulation is used by all location tracking systems. No GPS location is involved here, just because all cell phones need to be located, even the ones without a GPS feature, aka dumb phones. Other secure cell phones rely only on GPS mocking and data connection, which is actually a simple GPS faking through an installed app on the phone, which generates fake GPS location viewable by the phone user and other installed apps, used mainly for pranks and fun. GPS mocking cannot do the trick when it comes to professional location tracking. Once a GSM location is discovered, then a GPS position will be easily calculated by the location tracking system. A location tracking system will never directly extract GPS data off the phone! This can be done only by using so-called Govt grade spyware, which need to be installed on the target phone. The user of a Stealth Phone can choose which cell tower the phone is connected to. This way, any triangulation technique used to determine the location will give false results and thus a false location. The manipulated connection data is also stored by the mobile operator because the phone will send out the Cell ID which the phone is connected to. The distance between the actual location of the user and the location of the remote cell tower is between 1 and 10 km. If these data sets were subsequently requested by the authorities, all the location data would lead to false results and thus to the creation of a useless movement profile. The same when location tracking is performed in real time by a GSM Interceptor.



XCell Stealth Phones are equipped with patented technologies and offer a level of security that is currently unmatched by any other mobile phone.

For your real secure communications, XCell Stealth Phones offer you the highest possible protection against the risks of mobile phone interception and tracking. Stealth Phones protect conversations from being monitored by mobile operators, spy companies, skilled hackers, and abusive governments and guarantee that your calls, SMS and data remain 100% confidential and cannot be intercepted by third parties or IMSI catchers.

For those who recognise the need for totally secure communication, Stealth Phones are the perfect choice.

Contact

If you are interested in our solutions and demos, please contact us to arrange a meeting. We look forward to learning more about the challenges you face and will be happy to present our solutions to you in detail - in the current situation this can also be done in an online session.

+41 76 452 99 93

info@anti-interception.com

www.anti-interception.com

ECN GmbH
Ettenhauserstrasse 50
8620 Wetzikon ZH, Switzerland