What Are Common Techniques For The Invasion of Privacy For Individual?

McCann Investigations
1018 Preston St.
Houston
TX 77002

Table of Content

What Are Common Techniques For The Invasion of Privacy For Individual?

Invasion of privacy is majorly on it's way up. An annual study of internet security vulnerabilities released in 2011, showed that mobile vulnerabilities[1] **nearly doubled**, increasing by 93% in 2011, with a particular rise in threats targeting the Android operating system. It is estimated that worldwide mobile phone fraud will reach **$40 billion**[2] in a few years. This trend is certainly not limited to mobiles, it has also been seen in tracking vehicle GPS.

Privacy Invaders are located globally and can launch their attack from anywhere on the planet. For example, it has been reported that Russian hackers[3] are hoarding more than a **billion** in stolen passwords, username and more. **Cybercriminals** using spying tools could be raking in **20 times the amount** they spend on launching their attacks, according to Kaspersky Lab[4] experts.

Mobile phone monitoring

Although some cell phone spy programs are unobtrusive and can only be detected using professional services and instrumentation, sometimes there are noticeable signs that might cause concern. Certain indicators can raise suspicion on an eventual cell phone monitoring[5] [6] [7]:

- **trouble shutting down** – this is one of the most common issues with bugged cell phones. Background applications could significantly slow the process down.

- **experiencing odd phone behaviour** – from turning on unexpectedly, to making noises when not in use or installing programs on its own

- **battery rundown** – extra software activity, especially when running 24/7 may cause sudden changes in your phone's battery life

---

[1] Source: http://breakinggov.com/2012/04/30/mobile-hacking-nearly-doubled-in-2011/

[2] Source: https://supportforums.cisco.com/blog/12238621/mobile-phone-hacking-deadly-serpent-modern-era-technology

[3] Source: http://blackbag.gawker.com/heres-how-hackers-can-make-the-most-money-off-a-stolen-1619073981

[4] Source: http://articles.economictimes.indiatimes.com/2014-11-29/news/56561206_1_hackers-kaspersky-lab-experts-cybercriminals

[5] Source: http://spyzrus.net/how-to-tell-if-your-cell-phone-is-being-tracked-tapped-monitored-by-spy-software/

[6] Source: http://spyrambly.com/6-surefire-signs-your-phone-is-bugged

[7] Source: http://www.makeuseof.com/tag/6-signs-cell-phone-tapped/

- **high device temperature** – if your battery is in constant use, it usually becomes hot. If you notice your phone is warm when you're not using it, this may be because something is constantly running in the background

- **increased data usage** – some spy programs broadcast information directly using extra data, leading to increase in monthly usage

- r**eceiving coded text messages** – text messages containing random characters can sometimes result from communication attempts between your device and another

Some of these symptoms can be of course caused by overuse, bad connection or interference, but if they appear suddenly and constantly, they could be a manifestation of spyware on the cell phone. While cell-phone spy programs are versatile and complex tools for privacy invasion, most people are not aware of what they can actually do. A list of common features based on the most popular spy[8] applications[9] include:

- spy on calls, SMS, MMS

- spy on emails and instant messaging

- spy on passwords

- track GPS location in real time

- monitor internet use: social networks, downloads, etc.

- access contacts and calendar

- stealth camera – using the phone's camera to take a secret picture that is sent to your account

- geo-fencing – finding out when the user has entered or went outside a specific area

[8] Source: http://www.top10spysoftware.com/

[9] Source: http://www.bestphonespy.com/

Vehicle GPS tracking

Another common tool for individual covert surveillance is the well-known GPS tracker, most commonly used on vehicles. GPS technology market has seen a constant growth in recent years, with GPS device embedded in cars, motorcycles, mobile phones, tablets, computers, tools, equipment, hardware, dog collars and even pillboxes.

Opportunities to use this technology for undercover monitoring are following the same trend. GPS trackers are widely available for anyone to buy and install and specific features turns them into very effective spying tools. With prices ranging from $50 to $350[10], GPS trackers are proving to be one of the most cost-effective methods of technical surveillance[11].

For short term unobtrusive surveillance, **battery operated devices** can be easily planted on a car by any outsider. Quick **magnetic mounts** allow the devices to be placed on vehicles in **seconds**. Motion-activated devices are tracking only when the car is moving, extending battery life while live-view software receives data in real time, with position updates every few seconds. Some of the low-cost devices are data-loggers, with no real-time trace function, but only recording GPS data for retrieval. They are easily removed and leave no trace.

For more consistent surveillance, hard-wired devices can be used. They are connected to a *car's power source* and can stay in place for years with no maintenance. Given the fact that they are usually inactive when the vehicle is not moving, they are more difficult to detect and require professional services. For those who go through the trouble of planting a hard-wire device, it's common to combine GPS tracking and audio transmitter.

Professional bug or tracker sweep services use both physical inspection and hi-tech tools to detect and locate devices planted on or inside the target vehicle. A tracking device can only be installed by the owner of the car[12] and by law it cannot be installed into a vehicle owned by a different person. The same legal frame applies to mobile phone monitoring software.

Anyone who fears he or she may be the victim of illegal covert surveillance should seek professional tracker detection services with licensed investigators that are able to provide valid evidence and expert testimony in court.

[10] Source: http://www.brickhousesecurity.com/category/gps+tracking/vehicle+tracking+devices.do

[11] Source: http://www.gadgetsandgear.com/gps-tracking-devices.html

[12] Source: http://www.legalmatch.com/law-library/article/gps-tracking-laws.html

Why avoid "cheap sweep" and DIY sweep?

Professional TSCM services are costly to provide, with the cost of equipment, software and training easily adding up to hundreds of thousands of dollars. To illustrate, a comprehensive TSCM survey should include at least the following operations:

- **telephone instruments inspection** – some very effective bugs are placed inside telephone devices, using their internal infrastructure (microphones, power supply, telephone line for transmitting). Some are very compact and easy to overlook. The "infinity transmitter"[13], for example, intercepts all conversation in the vicinity of the telephone and remains active indefinitely, if not detected.

- **telephone Instrument analysers** are designed to detect bypass devices and wiring modifications inside the telephone instrument[14] and cost between $4,000 and $20,000.

- **telephone line analysis** – all devices and telephone lines must be tested for modifications that would allow the interception of conversations or room audio. A TDR[15] (Time Domain Reflectometer) can identify and locate faults on power and communication cables, with access to one end only.

Professional cable radar type devices range in price from $1,000 to $10,000.

- **Radio Frequency Spectrum Analysis[16]** – determining the source of each signal and also addressing special techniques such as carrier current, subcarrier, and frequency hopping, to detect transmitter bugs[17]. The price range for these instruments is $5,000 to $80,000[18].

- **Non-Linear Junction Analysis[19]** - detects the presence of electronics, regardless of whether the electronic target is radiating, hard wired, or even turned off. Allows for the efficient detection of all hidden clandestine devices including tape recorders, microwave transmitters, remote controlled transmitters, infrared or ultrasonic devices, as well as other non-linear junction devices that are possibly beyond the detection range of other test equipment.

---

[13] Source: http://spy-nexus.com/bug-guide/infinity-bug/

[14] Source: http://www.bugsweep.com/equipment.html

[15] Source: http://www.l-com.com/test-equipment-fault-mapper-pro-model-ca7027-telephone-cable-tester-graphical-tdr

[16] Source: http://www.reiusa.net/cgi-bin/main.cgi?action=viewprod&ct=products&pct=OSCOR%20Green&num=OSCOR%20Green

[17] Source: http://www.bugsweep.com/equipment.html

[18] Source: http://www.brickhousesecurity.com/product/oscar+green+tscm+spectrum+analyzer.do

[19] Source: http://www.reiusa.net/cgi-bin/main.cgi?action=viewprod&ct=products&num=ORION%202.4

These devices range in price from $16,000 to 30,000[20].

- **physical inspection** – Thorough inspection of power outlets, light fixtures, wall cavities and other possible risk areas (especially areas connected to power supply) to ensure no hardwired bug is planted as well as inspection of all physical items to detect possible battery operated bugs. Professional investigators should use video cameras to inspect unaccessible cavities.

These types of video camera can cost several thousand dollars[21].

- **voice-over Internet Protocol (VoIP) systems[22]** – checking internet protocol (IP) packet traffic on VoIP phones and systems to identify possible cyber bug. Performing multiple tests on multiple phone lines allows investigators to quickly identifying any anomalies.This kind of analysers can cost up to $20000[23].

- **malware, spyware or computer surveillance detection** – using latest testing technologies to identify stealth cyber attacks. Keeping this kind of resource updated is also very costly for service providers, as the spyware world is very dynamic.

Another issue is the cost of professional training and certification for TSCM investigators, which is an ongoing cost for companies who want to keep a competitive advantage and offer high-end services.

Anyone looking for TSCM services should have a **realistic representation** of the value of the available options. A few simple questions should help clarify if a prospective service provider is as professional as claimed:

- what **equipment** are they using to identify bugs?

- is the **company licensed** and insured?

- is the **personnel qualified and certified**?

Service providers who fail to keep their capabilities updated are only offering their clients a false sense of security, which may prove unprofitable on long-term. Being suspicious of unauthorised surveillance is actually preferable to feeling safe after an incomplete bug survey.

[20] Source: http://www.bugsweep.com/equipment.html

[21] Source: http://www.brickhousesecurity.com/product/rei+video+pole+camera.do?sortby=ourPicksAscend&page=2&from=fn

[22] Source: http://www.reiusa.net/cgi-bin/main.cgi?action=viewprod&ct=products&pct=TALAN&num=DPA-7000

[23] Source: http://www.spybase.com/product-p/dpa700.htm

Why McCann's is unique as they offer both cyber and physical TSCM.

1. **Most companies do physical TSCM only.** Companies like tscmamerica.com are basically ex-federal officers and not exposed to digital Technical surveillance counter-measures.

Covert technical surveillance has been used ever since technology allowed this kind of operations, as one of the most effective ways to gather sensitive information from unsuspecting targets. With technological development, as cost dropped and efficiency increased, there is a growing trend of unauthorised surveillance of industrial and individual targets.

Technical surveillance counter measures emerged as a natural consequence. Well equipped and trained professional service providers are now able to detect and locate most planted **physical bugs**: microphone or video camera recorders or transmitters, phone taps, GPS trackers and other hardware interception devices.

Bug detection techniques are based on **finding infrastructure irregularities** using various analysers and detectors: Time Domain Reflectometer, Non-linear Junction Detector, Spectrum Analyser, Oscilloscope, etc. This type of detection services is now considered the classic TSCM approach.

2. A bug can be **digital or physical.** i.e. these listening devices can be physical or in the form of software within the mobile.

Over the last decade and more acutely in the past few years, the **focus shifted** from conventional hardware bugs to **cyber bugs**. These are software programs that target IT equipment and use its capabilities to secretly intercept and transmit information. Cyber bugs are very effective as they can either retrieve information as classic bugs do (content and activity of a device) or simply turn the whole **device into a spying tool**, by using its microphone, camera, GPS, etc. If we count the fact that mobile devices are always on the move with their owners, cyber bugs become even more frightening.

In other words, cyber bugs do not have a hardware body but can do the work of a hardware bug and much more. Not being an actual device to pinpoint, cyber bugs are often **difficult to identify and locate.** This can be accomplished only by detecting anomalies associated with digital media, GSM, Wi-Fi, Bluetooth or local networks.

These mediums, along with the actual devices can be scanned in order to identify potential pathways for cyber bugs. A Cyber TSCM service provider works closely with the **IT Security department** to eliminate cyber threat by:

- **network mapping and monitoring** to assess possible threats

- **determine anomalies** in cellular and Wi-Fi signals

- **analysing network hardware** like individual networked computers, wireless access points, switches, routers, power sources or cables

- **monitor traffic and information flow** using specific test programs

Why is it advantageous to have one company doing both physical and digital TSCM

The physical and digital realms are more than obviously **interconnected.** Each entry point represents a vulnerability from one side to the other. IT devices like computers, tablets, mobile phones have both physical and digital components and huge surveillance capabilities (with microphones, camera, transmitters, GPS, etc).

For example, the growing "**bring your own device to work trend" (BYOD)** trend allows the use of **unregulated personal devices** that could pose a Cyber security threat to the entire network of a company.

A comprehensive TSCM survey should take into account both physical and digital infrastructures and demonstrate a holistic view when assessing potential threats.

A company that develops its conventional TSCM services to integrate the legitimate need for cyber security shows determination to **deliver high-end services and keep competitive advantage**.

Why McCann's REI trained technicians and gear is better than competition

REI is a world leading manufacturer of technical surveillance countermeasure equipment. REI customers include Government agencies, Law enforcement organisations, Corporate Security personnel, and TSCM (Technical Surveillance Countermeasure) professionals that have a need or responsibility to protect sensitive information.

Founded in 1983 in Cookeville, Tennessee, REI was one of the first companies to introduce a Non-Linear Junction Detector (NLJD) in the US (http://www.cryptomuseum.com/df/rei/index.htm) and claims to be the largest manufacturer[24] of such equipment in the World. All[25] design and manufacturing work is done on site, in Algood, Tennessee, focusing on quality and complexity instead of production volume.

[24] Source: http://www.prweb.com/releases/2011/04/prweb5237004.htm

[25] Source: http://depreciated.ucbjournal.com/news.php?id=3115

REI also operates the largest[26], unclassified, commercially available TSCM training centre in the world, using state of the art technical security equipment. They train TSCM professionals in overall surveillance countermeasure practice or certification courses for using their equipment. The REI training centre is clearly following the **big trend** in the surveillance technology, with more new courses focused on Digital Electronic Surveillance Counter Measures.

In over 3 decades of security technology development, REI has always proved to be a **reliable partner** for both government and private sector clients as well as one of the leading manufacturers in the industry. Using REI technology and know-how has become a guarantee for quality TSCM services.

[26] Source: http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/REI.pdf


MCCANN INVESTIGATIONS
EST. 1984
TOTAL SECURITY SOLUTIONS