I'll be Watching You

Henry B. Wolfe[1]

Abstract

We take for granted every day that we are safe from any given risk because we are protected by various standards, statutes, laws, and the goodwill/honesty or people globally. The mobile phone, for example, touches almost every part of our daily lives. There are currently more than 8 billion connections and almost 5 billion mobile phones in use around the world. It is really nothing more than a small computer with a radio transmitter and receiver and other communications devices (Wi/Fi, Bluetooth, etc) integrated into it. Mobile phones may also have the ability to record and store photos, videos and sound. Most have a built in Global Positioning Satellite System capability. Each of these capabilities may result in various risks. Every generation of mobile phone has expanded its capabilities and connected to the Internet in addition to normal telephone functions. It has become the most effective surveillance device ever conceived by man.

Along with these phone capabilities come a number of risks. Some of these are usually associated with using the Internet, so mobile users are exposed to malware of various kinds and being hacked for malicious purposes. However, there are other more insidious less known risks. The purpose of this presentation is to discuss current general surveillance techniques associated with mobile phones, the Internet, and other avenues of collecting evidence. Some of the discussion will cover communications interception, location logging and tracking, and bugging. Many people using mobile phones are not aware of these threats, or assume it only happens in other countries. They assume their service provider (Internet and/or mobile phone) has put measures in place to eliminate risks as well as protect their privacy (by the use of cryptography). 100% safe Internet and mobile phone use will unlikely ever be possible. This presentation will graphically portray and clearly describe example aspects of surveillance techniques in defined language that non-technical people will understand. Explanations as required will be provided in the general discussion afterwards.

1. Introduction to Surveillance (what's it all about?)

"The word *surveillance* comes from a French phrase for "watching over" (*sur* means "from above" and *veiller* means "to watch")"[2]. Watching over has many different objectives. For example we watch over but are not limited to:

1. Our children until they are old enough not to need that sort of care and supervision.
2. Our possessions to ensure that no one takes them from us.
3. Our partners to ensure that they are protected and secure, and also to ensure that they are faithful/loyal.

In the context of this paper we are concerned about the kinds of surveillance techniques that we might use or encounter in civil cases – some of which are legal and some may not be. It is important to understand that just because a technique is not legal does not mean that it will not or cannot be used. Indeed illegal techniques are in use all of the time.

[1] Associate Professor – University of Otago, PhD, Otago Business School. Almost 60 years as an ICT professional – the last 35 or so devoted to security.
[2] **Wikipedia** – explanation of the origin of the word *surveillance*.

Civil cases may be about money or abuse or other issues, but they all have in common the need to collect evidence that will support or refute a given claim or assertion. In some instances the individual may be in a position to collect some evidence. It may additionally be necessary to engage a professional (private detective) to collect evidence that might be difficult or impossible for the average person to collect. At the end of the day, whatever evidence is collected will be scrutinized, and in a court of law a determination will be made as to whether it will be allowed into any formal proceeding. In most cases illegally gathered evidence will be disallowed.

2. Likely types of surveillance techniques used in civil cases

There are a great many surveillance techniques. Large and complex books have been written about them. Some are so sophisticated that they are only used by the law enforcement or the intelligence community. Just because one of these techniques could be used successfully in a civil case and produce relevant evidence does not mean that you may be able to use it. This is due to any number of factors such as legality, expense, level of required technical expertise and equipment availability, etc. Eliminating these specialised or sophisticated techniques does not make it impossible to collect relevant and legally obtained evidence through other surveillance techniques. Some of these are described below.

3. A discussion of surveillance types:

a. Listening devices

i. Introduction

The devices and techniques described below are for the most part illegal to use. Unless you have a warrant, evidence captured by these methods may not be acceptable in a court of law. However, the notion that they will not be used because they are illegal is naïve. Often information obtained in this way can be useful in leading to or finding other evidence through legal means.

ii. Radio


Make your own FM bug

Listening devices are most commonly found to use radio as the broadcast medium to transmit sound to the person(s) or entity that is undertaking the surveillance. These devices are varied in sophistication from simple FM (Frequency Modulation) band to high or ultra high frequencies. FM typically broadcasts in the 87.5MHz to 108.0MHZ range.[3] It is commonly used in car radios and alarm clock radios. FM is used to broadcast the sound a listening device (bug) picks up and is simple, cheap, and effective. An FM bug can be purchased for around $20 and up or if you're an amateur electronic hobbyist, plans can be purchased. An example of these devices is baby monitors. However, selling bugs can be illegal in some jurisdictions.

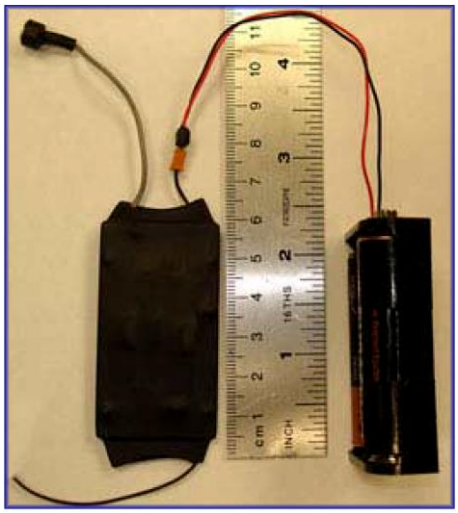
There are various types of radio bugs. The FM bug described above is the simplest but there are others that make use of the different spread spectrum techniques such as frequency hopping, direct sequence, time hopping, and burst. The use of spread spectrum requires that both transmitter and receiver be synchronized. As the communication

[3] The **International Telecommunications Union** (ITU) regulates generation and transmission of radio waves internationally. It has divided the radio spectrum into 12 bands ranging from 3Hz (Hz – a Hertz or one unit of frequency at one cycle per second) to 3000GHz. FM radio is in the VHF band (ITU #8) and is normally found from 87.5MHZ to 108.0MHZ frequency range.

technique becomes more sophisticated the cost of production increases accordingly. The reason for the increased sophistication is that each improvement makes detection more difficult.

Rigol Spectrum Analyzer

Detection of radio bugs is normally done using a radio spectrum analyzer. This device cycles through the radio spectrum (typically from 9 KHz to either 3GHz or 6GHz) looking for radio broadcasts. When one is detected, the analyzer alarms and displays a spike on the video screen describing the exact frequency found. An FM bug's detection is fairly simple since its signal is transmitted at one frequency and with a fixed time interval. Spread spectrum detection of such a bug is more difficult since the time and/or the frequencies are constantly changing.


Controllable Burst Transmitter

With a burst transmitter, sound is recorded in digital memory capacity and as the memory reaches a threshold trigger, the device transmits a very high speed burst of digital radio traffic, clears the memory, and continues recording. In this case the transmission is only active for a few milliseconds and almost impossible to detect with a spectrum analyzer. The price could be as much as $7,000 for a used Russian model and up to $35,000 for a new one.

iii. Carrier Current

Most electronic hobby shops carry plug-in house intercoms. These are not radio devices. This communications technique is referred to as carrier current. It uses the house wiring to provide electric current for any devices plugged in to it. It is worth mentioning that a signal transmitted through carrier current will travel over electric supply wires within the building and beyond until it reaches a transformer. If that is at the end of your street, then every building in between could, with the same model intercom, listen in to any sound being transmitted over this channel. This technique is also used as a bug and would be mounted in a power receptacle.

iv. Light (laser, lighting device variation, etc.)

Sound is nothing more than the modulation (vibration) of air. There are many ways to pick up sound. One is called the Buran[4] and uses a laser to reflect off a window of the room where a conversation of interest is taking place. The reflected laser light will be transformed by the minute modulation of the glass in the window, with the modulation reflected back and translated into sound.

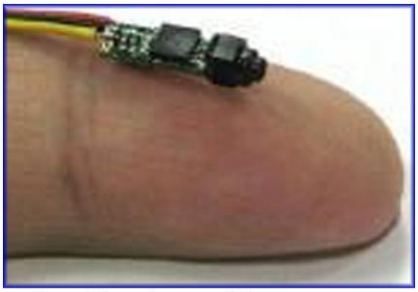
Another light capture method uses a device placed between a bulb and the light socket. It has a microphone that varies the power to the bulb, is not perceptible to the eye, but easily

[4] **Buran** – this surveillance technique was invented in the mid-1940s by a Russian born in St. Petersburg, Russia: Léon Theremin. The original device used a low power infrared beam. Later versions use a laser. Theremin also invented the basis for today's RFID (Radio Frequency Identification) technology used in most credit/debit cards as well as RFID passports.

translated back to sound using specialist light detectors. A limitation is the line of sight to the lamp or light source in order to capture the modified light.

An interferometer device coupled with other electronic equipment is used to measure the difference between the original and the reflected signal to translate into sound.

v. Video



Small colour video camera

Video surveillance is everywhere today. It is found in stores, in public places, in malls, parking lots, and just about anywhere that needs to be guarded. Miniature transmitting video cameras are easily obtained and provide another surveillance technique. These must be placed in various ways. A pin hole lens camera allows it to be placed with the visible lens only about the size of a pencil lead. These are often placed in the ceiling. Infrared cameras can be hidden behind infrared filter material. The eye cannot see through that material. The filter material looks like black plastic and cameras may be hidden behind it. Examples are inside exit signs, alarm radios, wall clocks, smoke detectors, intruder detectors, and anything where black plastic can be used in an item's construction. Video transmitters can be detected using the standard spectrum analyzer and make a very distinctive stuttering sound.

vi. Specialist Microphones

There are several types of microphones with a variety of purposes. When the target is in the open, a shotgun, Gatling, or parabolic microphone can be used. These are very hard to hide and limit capture to around thirty metres. If the target is facing away from these directional microphones it may not be possible to capture their conversations.

If access to the target's premises is possible, then a contact microphone or a spike microphone can be put in place. A contact microphone is placed on a wall's surface and if the conditions are right can pick up sound on the other side of the wall. A spike microphone requires drilling a hole in a wall of the target location and inserting the spike. It can also pick up sound in the room at the point of the spike. These are most often hard wired to a listening station and do not use a radio transmitter.

vii. Land Line Bugs

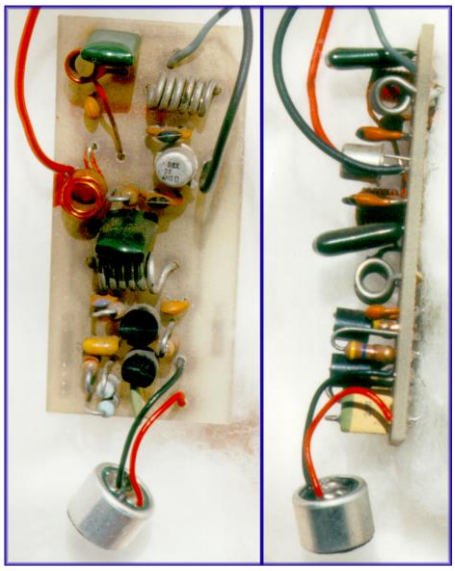
Land line phones are easily bugged. There are different forms: infinity, induction coil, using the second wire pair.

- An infinity bug must be installed on the phone itself. The handset microphone can be activated without the phone ringing. Sound in the room is then picked up.
- An induction coil when placed next to the phone line can pick up electromagnetic radiation from the line and translate that back into sound.
- Every land line has two pairs of wires. Only one pair is used and the second set could be connected to the handset and activated at will.

Finding these bugs requires a physical inspection of the phone, wires in between, and connections to the telephone pole. Telephone bug detectors cannot always find these types of surveillance devices.

In Summary

These are some of the most common surveillance devices used for capturing sound. Most can be purchased over the Internet. The quality may vary but they do produce results. You are probably asking yourself why bugs? Bugs are only used in Washington, London, Moscow and the like. Well that's not actually true. The photo to the right shows an FM bug found in situ in Dunedin during a routine installation of a new security system. This was most probably made from a kit or electronic hobbyist plans and cost about $15-$20. It's effective range is beyond one and a half kilometers in the open and a few hundred or more meters where it was placed. In this case the bug was placed in the crawl space above the ceiling directly over a manager's desk.



Dunedin: FM Bug

b. Biological

i. Trace evidence

Trace evidence consists of physical material such as fingerprints, skin, hair and other things that can only come from a specific person. While this is mostly not a surveillance activity, it never the less plays an important part in placing an individual at a location.

ii. Biometric Identification

Biometric identification is used in various ways to identify individuals. For example, when you pass through Immigration & Customs your face is scanned and that scan is compared to a database of persons of interest. This technique can also be used in the analysis of video footage where an individual needs to be identified.

c. Computer

i. Internet

The Internet can be a source of important evidence. People use it for many kinds of things. If, for example, a spouse had hypoglycemia, information about how that condition could be exacerbated can be found on the Internet. If someone were to use that information to hurt their spouse, it is possible to find evidence that the perpetrator searched for that topic on the Internet and it may go some way to prove motive and opportunity.

The Internet can be used to move money and assets around. In a civil case, knowledge of those kinds of movements would be central to any financial agreement entered into.

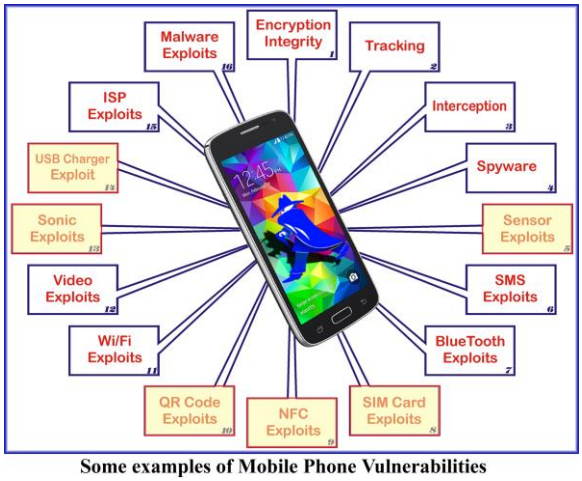
In marital disputes, infidelity communications may provide evidence central to any agreements entered into.

d. Mobile Phone

Introduction

The mobile phone is the most effective and efficient surveillance device ever conceived, and constructed by man. That's a pretty sweeping statement but I believe that after you consider the following that you will also agree. As well as being able to be attacked individually, many features described below can be compromised by the purchase and

installation of a single product, and are freely available from the Internet – at a price (see ***section iv*** below). Of course using one of these products is most likely an offense. To reiterate, just because it may be illegal does not mean that it will not be done.



Some examples of Mobile Phone Vulnerabilities

i. Mobile Phone Encryption

Mobile Phone Service Providers (MPSP) have added protection of communications in their systems through the use of cryptography. However, research within the cryptographic community has shown these cryptosystems to be either deliberately weak (as proven to be the case within the GSM system) or poorly conceived as shown by Biham and Dunkelman in 2000[5]. The cryptographic functionality often can be thwarted through various technical means – and in some cases without the application of cryptanalysis.

Examples of flawed or weak cryptographic protection provided within various mobile phone systems include but not limited to:

In March 1997 the Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) systems were compromised by Counterpane Systems[6]. The Collision Eliminating Multiple Access (CEMA) cipher, a 64-bit algorithm, used in some early mobile phones was shown to be weakened to an effective length of 24 or 32 bits (trivial to crack).

The Global System for Mobile Communications system (GSM - formerly known as Groupe Spécial Mobile - a common and popular moblie phone system) has a long history of successful attacks. Two researchers (Biham & Dunkelman) discovered that the A5/1 (a block cipher) algorithm's GSM 64 bit key was deliberately designed to be less secure – "In practice, A5/1 was always used with only 54 bits of key, with the remaining 10 bits set to zero."[7].

[5] Biham, Eli & Dunkelman Orr, December 2000, *Cryptanalysis of the A5/1 GSM Stream Cipher, Progress in Cryptology* – INDOCRYPT 2000, Bimel Roy & Eiji Okamoto – editors, Springer, India, ISBN:3540414525.
[6] Counterpane Systems, 20 March 1997, Press release → www.schneier.com/cema-press.html
[7] Biham, Eli, Dunkelman, Orr, 1999, *Cryptanalysis of the A5/1 GSM Stream Cipher*, a research paper supported by the European Union fund IST-1999-12324 – NESSIE and by Technion-Israel Institute of Technology's Chais' Excellence Program.

A brute force attack (also known as an exhaustive key search) against a strong algorithm means testing every possible key until the correct one is found. A comparison of key spaces follows:

A5/1 - 2^{64} = the total possible key space is:

18,446,744,073,709,600,000 unique keys.

Weakened A5/1 – 2^{54} = the total possible key space is:

18,014,398,509,482,000 unique keys.

The **difference** between the two is:

18,428,729,675,200,100,000 unique keys.

The remaining key space represents 1/10th of 1 percent of the original 64-bit key space. Anyone could reasonably conclude that this constitutes a significant reduction in the security provided by the original GSM A5/1 crypto algorithm.

NOTE: To put this into perspective, in 1998 Cracking DES[8] was able to solve a DES (the American Data Encryption Standard – a 2^{56} bit key space: 72,057,594,037,927,900 unique keys) encryption in a few hours. Processing power has improved in the past nineteen years since that occurred.

The 10 bits always set to zero flaw has since been corrected but it is evident that the original intention was to weaken the security of the voice encryption capability of GSM. This issue is really academic; illustrating the fact that strong encryption could have been used but instead it was not. In December of 2000 the A5/1 crypto algorithm of GSM was defeated (shown to be solvable in a trivial amount of time) by Biryukov, Shamir & Wagner 2000[9] and separately by Biham & Dunkelman 1999.

Mobile Phone Encryption – Notification

In the GSM specification there is a provision for notifying each mobile phone user when their conversation is not being encrypted. The GSM Technical Specification[10], on page 15 states: "The ciphering indicator feature allows the ME (Mobile Station – mobile phone) to detect that ciphering is not switched on and to indicate this to the user, as defined in GSM 02.09"[11]. However, GSM Technical Specification, on page 8 states: "This ciphering indicator feature may be disabled by the SIM)."[12].

Paget states the corresponding tag on the Subscriber Identity Module (SIM)card is usually disabled and that means the user's phone will not inform them when communication is not being encrypted[13]. The rationale for mobile phone service providers disabling this feature is not known. If an interception is in place that disables the phone's encryption, that fact will not be detected by the GSM notification feature and the user will not be informed.

Mobile phone service providers manage a communications network. Part of that administration is network traffic analysis. This allows a MPSP to upgrade bandwidth and

---

[8] Gilmore, John, Electronic Frontier Foundation, 1998, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*, Electronic Frontier Foundation, April 30, 1998, ISBN‑10 1565925203.

[9] Biryukov, Alex, Shamir, Adi, Wagner, David, 27 April 2000, *Real Time Cryptanalysis of A5/1 on a PC*, Cryptome, , the Weizmann Institute, Israel.

[10] GSM 02.07 V7.1.0 (2000-03), Technical Specification, ETSI, Valbonne, France, 2000.

[11] GSM 02.09 V6.1.0 (2000-02), Technical Specification, ETSI, Valbonne, France, 2000.

[12] GSM 11.11 V5.0.0, Technical Specification, ETSI, Valbonne, France, 1995.

[13] Zetter, Kim, 2010, *Hacker Spoofs Cell Phone Tower to Intercept Calls*, Wired, July 2010 → wired.com/threatlevel/2010/07/intercepting-cell-phone-calls/.

other elements of their network before a mobile's communication saturation threshold is reached. These providers use cell tower triangulation for this purpose and record every phone's location when polled. The information is recorded for use in traffic analysis and is a necessary management tool.

ii. Mobile Phone Tracking

Most mobile phones now have GPS functionality and that makes tracking a specific phone much easier and more accurate. Both offer the potential for an attacker to track the current, and potentially historical, location of any targeted mobile phone. That information may be vital for locating someone in an emergency and the requirement for this capability has been legislated in some jurisdictions – such as in the USA.

On the other hand, this information could be used as evidence to prove where the holder of the phone was at any given time. Normally this information is not available to the public. It must be obtained by providing the MPSP with a warrant issued by an official judicial authority after the presentation of evidence of probable cause to justify the issuance of the warrant by that judicial authority.

Mobile phones typically have a GPS as a built in device. This communicates with the worldwide Global Positioning Satellite System and creates longitude and latitude coordinates of the phone's location – depending on surroundings, up to an accuracy of a 4.9 metre radius. These updated coordinates are available every cycle (from 1 to 5 times per second) to the phone for whatever purposes that have been configured. This information is updated in regular intervals. The MPSP, as a part of routinely managing their communications network, records the mobile phone's location. This historical information is kept and used for network performance analysis. Some applications require permissions to also capture GPS location coordinates and transmit them back to the application's originators. The requirement for this permission is dubious at best. In most cases the user is normally not informed that they are being tracked.

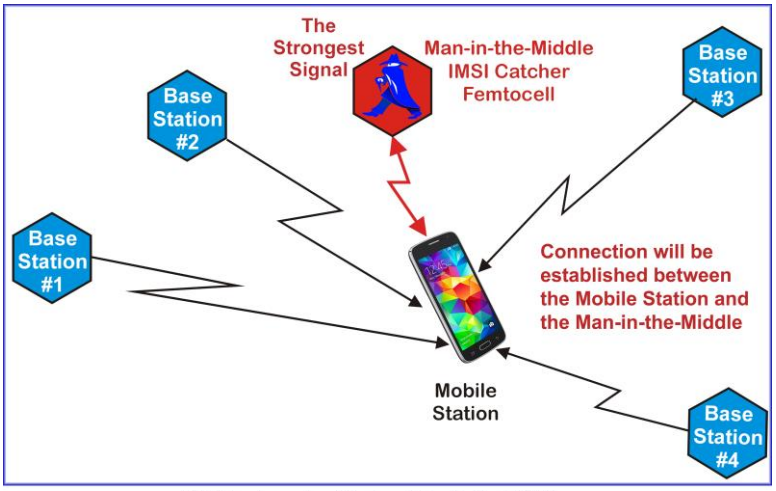
The historical location data is available from the MPSP when provided with a duly executed warrant. Applications and spy software that capture this information usually do not ask permission (except as a requisite for installation).

A further important use is that unless otherwise configured, all images captured with the mobile phone's cameras have included in each .JPG image file the time, day, and physical coordinates specific to that image. This may also be a potential source of evidence.

iii. Interception - IMSI Catchers

In the context of this paper, interception refers to communications that are compromised at some point along the communications channel. Often, but not in all circumstances, this facilitates a "man-in-the-middle" attack where the attacker controls both sides of the communication. An attacker can either listen in and gather information, or take a proactive role and inject information into either or both sides of the communication. The targets would not be aware of this breach in their communications channel/process.

The IMSI (International Mobile Subscriber Identity) is the number used by the MPSP to identify valid subscribed users and is stored on the SIM card. It forms a part of the initial handshake between the user and the cell tower (BS = Base Station). An IMSI catcher provides eavesdropping and surveillance capability by intercepting this number and using it in a man-in-the-middle attack. The IMSI catcher masquerades as a Base Station. For example: Vodafone Sure Signal Femtocell - NZ$249 including GST can be modified to be an IMSI catcher.



Mobile phone handshake - Man in the Middle

Every Mobile Station (MS) has the requirement to optimize its reception. Therefore if more than one Base Station is accessible, the MS will choose to connect to the one with the strongest signal.

An intruder (IMSI Catcher, Femtocell) merely has to place themselves between the cell tower with the strongest signal and the target phone generating the strongest signal. During this handshake connection sequence (after the IMSI number has been verified), the BS instructs the MS to use a specific encryption algorithm: A5/0 or A5/1 or A5/2. In this case the man-in-the-middle instructs the MS to use A5/0 – meaning no encryption. After that the man-in-the-middle sees traffic in clear form and just relays communications between MS and BS.

iv. Spy Tools

The Internet is a source of specialized software that can accomplish various capabilities[14]. These surveillance tools have a varied number of attributes from complete control of the target phone giving the ability to listen in, see texts, locate the phone, see all incoming and outgoing phone numbers, copy files, initiate a roving bug, etc. Some display an icon that designates that the phone is being monitored and that icon cannot be removed. Others have subsets of the various capabilities mentioned above. The prices range anywhere up to $500-$600 per year. At this time there is no fully automated identification or detection of these surveillance tools being installed on a given phone. Installation may be accomplished through several vectors and does not always require physical control of the target phone. In many jurisdictions this type of surveillance tool would be illegal to use.

Bugging

Mobile phones can be configured to become a bug (listening device). This technology has the ability to activate the mobile phone's microphone and to be able to listen to whatever it picks up – from wherever the mobile phone is located. This is not the only

[14] Some examples are: ***Appmia, Flexispy, Mspy, PhoneSheriff, Spyera, Inteceptor SpyPhone***, etc. There are many more.

way that a mobile phone can be turned into a bug. The many applications, found on and available from the Internet, can provide the same functionality from wherever the attacker is located – virtually anywhere in the world. Mobile phones can also be easily configured by their owner to act as a bug and left to listen in to whatever sound may be heard in the immediate vicinity. That requires no special device or software.

v. SMS Exploits - Over-The-Air Programming

Simple Messaging Service (SMS) is a method for sending short messages to the mobile phone. Normally these are used by the owner for texting. Service SMS messages are designed to enable MPSPs to update the client phone's operating firmware (aka device configuration). It may be possible, via SMS, to configure a mobile phone so that each entering and exiting phone call will be silently conferenced with the third party (the SMS originator). It is possible to send a silent SMS that will return the GPS coordinates of the target phone at that instant. SMS has begun to be exploited. There will very likely be more developments in this technical arena.

vi. Targeted Acquisition – Bluetooth

Mobile phones can store all sorts of personal information as previously outlined. Bluetooth is an open wireless technology for the exchange of data over short distances - it is just radio communication over a specific frequency band width (2.40-2.48GHz). Its functionality is implemented in most mobile phones and enables functions such as hands free cable-less communication, backing up to the desktop, and other types of file transfers.

If the user's phone has Bluetooth and it is activated (that channel can be monitored by an *Ubertooth One*[15]), all of the information stored on the targeted phone may be downloaded by an intruder from more than a kilometre away. The user will not be aware of this action until the information downloaded is used to their detriment. John Hering, the builder of *Flexilis,* has published a "how to" set of plans[16]. The plans for building the device are freely available from the Internet. That means that other interested parties will use this technology to their advantage.

vii. Wi/Fi Exploits

Recently a New Zealand couple carried out some on-line banking using available free Wi/Fi in San Francisco or Los Angeles. When they returned to New Zealand a six figure amount was withdrawn from their account using details captured over that Wi/Fi connection. Using "free" Wi/Fi wherever you happen to be should be done with great care.

It is possible to use a network of Wi-Fi base stations in a limited area to pinpoint the exact location of a targeted phone if Wi-Fi is left activated on the phone. It should be turned off if not in use but in practice most people do not do that. This would be an expensive and complicated surveillance technique for tracking someone.

---

[15] Ubertooth, 2013, - Bluetooth monitoring device → ubertooth,sourceforge.net

[16] Cheung, Humphrey, March 08, 2005, *Bluesniper – a device designed to target and capture data from Bluetooth enabled mobile phones from a distance of a kilometre or more.* Plans in two parts available from the internet:
Part 1 → www.smallnetbuilder.com/content/view/24256/98/
Part 2 → www.smallnetbuilder.com/content/view/24228/98/

viii. Video Exploitation

PlaceRaider[17] is a proof-of-concept Trojan, developed at the Indiana University in concert with the U.S. Naval Surface Warfare Center, that demonstrates the invasive potential of visual surveillance malware. This application, once installed on a targeted mobile phone, captures an image using the phone's built in camera. These images are collected, analyzed and arranged into a 3D model of the environment. Anything in that environment can be further analyzed – such as documents that may be readable, other items or individuals of interest.

Video Exploitation of GPS Functionality

Smart phones with GPS functionality and cameras provide the default of inserting physical longitude and latitude coordinates into the metadata which is a part of the JPG image files created by the phone's camera. Images captured in this way and shared with others can be probed to find out where and when the photo was taken.

Not all social networks clear this metadata before putting images up on their website. This information could be useful to a burglar or stalker. The GPS feature can be turned off for the camera.

ix. MPSP Exploits

Voice Mail

The MPSP as a matter of course, track and record every mobile phone in their domain from tower to tower.

Individual mobile phone location information is available to Law Enforcement and potentially others who are willing to find and pay the right person to get it.

It is possible to obtain (from the MPSP) cell tower dumps. These contain date, call length, whether the call was inbound or outbound, or went to voicemail, mobile number and location, and whether the mobile phone was in motion or stationary.

With a little thought one can imagine how this information could be used.

Voice Mail is recorded and held on the MPSP's servers and can be browsed by Law Enforcement, without a warrant in some jurisdictions and without the user's knowledge. It can also be browsed by whoever the MPSP will allow, also without a user's knowledge. This data once recorded on the MPSP's servers is almost always retained.

x. Malware Exploits

Spam, Viruses, Worms, and adware are all unsolicited, unwelcome and unnecessary to the normal operation of the mobile phone. Spam, phishing and the like are attempts to encourage the user to give up personal information which, in most cases, is not in their interest. Viruses, Worms and other attack software are designed to do damage or to take over the user's machine.

Mobile phone operating system's APIs, provide applications with large amounts of information about users. Applications, in addition to whatever service their primary

[17] Templemany, Robert, Rahmany, Zahid, Crandally, David, Kapadiay, Apu, 2013, *PlaceRaider: Virtual Theft in Physical Spaces with Smartphones*, Indiana University and The US Naval Surface Warfare Center, September 27, 2012 → arxiv.org/pdf/1209.5982v1.pdf

purpose offers, may also provide a vector for installing malware or for reporting users' activities back to the application's master. Many applications take advantage of the permissions system and at installation time the user will be asked to allow access to various services that the application does not actually need to perform the stated/expected service. Most applications ask for various permissions. Malware applications often ask for specific permissions such as access to GPS or permission to send SMS. Those attributes have been put forward as potential identifiers of malicious applications by a group at Berkeley[18].

xi. Voice communications

While voice communication is, as a matter of course, encrypted (to protect the communication while being transmitted), the simple fact is that the encryption in place has been shown by a number of different credible cryptanalysts to be weak and easily defeated[19]. Since communications via mobile phone are radio transmissions and can be captured from the ether, cryptanalytic techniques can then translate those captured transmiossions into understandable voice communications.

Another technique to accomplish the same result is to impersonate a cell tower (becoming the man in the middle) and turn off encryption and listen in as discussed above.

xii. Text

Texting is one of the most used features on mobile phones. An application designed to capture these can send them to its master. More than 50% of all applications that users install on their mobile phone are reporting activities back to their master – for example: *Super-Bright LED Flashlight* asks for 20 permissions before you install it. Why would your flashlight need to have access to your GPS location? Most phone applications have hidden agendas of one kind or another.

Trap & Trace (incoming and outgoing telephone numbers)

Numbers of all incoming and outgoing calls can be captured. This can be done via an application or via one of the surveillance products listed in footnote number 14 on page 9. This captured information may be relevant to a case.

xiii. Location

Mobile phones have built in GPS which constantly provides the geographic location longitude and latitude coordinates. With this information the phone can be tracked at all times – anywhere in the world as long as there is mobile coverage. This information is also recorded by the MPSP and may be obtained with a warrant or court order. Knowing where the phone is usually tells you where the owner is. Turning the mobile phone off may not stop this function from working.

[18] Felt, Adrienne Porter, Finifter, Matthew, Chin, Erika, Hanna, Steven, Wagner, David, 2011, *A Survey of Mobile Malware in the Wild*, SPSM'11, University of California at Berkley, 17 October 2011, ACM 978-1-4503-1000-0.

[19] **A5/1 encryption algorithm**, used by GSM, was cryptographically defeated in December 2000 - Biryukov, Shamir & Wagner and separately by Biham & Dunkelman.

xiv. Probing stored contents

Gaining access to a mobile phone makes available any information residing on that phone. This information can also be captured via electronic forensics. Access may be gained through Bluetooth and other remote access methods. Once access is gained, the entire contents can be copied without the owner's knowledge.

4. Potential sources of evidence through the surveillance or data gathering of others

a. The MPSP

The MPSP, as mentioned earlier, maintains a running history of the physical location of mobile phones identified in their mobile network as well as all voice mail for every account. This information may be obtained with a warrant or court order.

b. Private detective

Private detectives may be engaged to perform physical surveillance as well as searching other sources for relevant evidence. Depending on their methods, evidence captured may be inadmissible in court proceedings. When a private detective is used, the hirer must be clear about what they are looking for and any limits that they would impose on the detective's search activities.

c. Police

Various forensic capabilities in the realm of mobile phones and computers can be found with the Police. If the matter is criminal, then their involvement will likely be required. There are also private electronic forensic firms that provide such services. A thorough electronic forensic investigation is time consuming, expensive, and cannot guarantee the discovery of relevant evidence.

5. Summary

This paper has discussed a number of different surveillance techniques. In any given adversarial situation, the parties will attempt to discover whatever information they can that is relevant to their case. That information may be captured by one or more of the techniques described in this document. There is no guarantee that any of the methods described will be successful in obtaining that "smoking gun" evidence. Moreover, what has been discussed is only a subset of the actual kinds of surveillance that could be attempted. It is important to remember that just because it may be illegal does not mean that a surveillance technique will not be used.