McCann
INVESTIGATIONS
Information | Insight | Influence

Case Study: Cyber Stalking and Spyware in Divorce Cases

McCann
INVESTIGATIONS
Information | Insight | Influence

Company Profile

McCann Investigations is a full service private investigation firm providing complete case solutions by employing cutting-edge computer forensics and traditional private investigative tools and techniques. For 25 years, McCann's investigators have worked in the public and private sector encompassing law enforcement, physical and electronic security and computer forensics.

McCann works with law firms, financial firms, private and public companies and individuals in cases including contentious divorce, child custody issues, fraud, embezzlement, spyware/malware detection, civil and criminal background investigations, and due diligence.

McCann Investigations tools include:

- Computer Forensics
- Mobile Device Forensics
- Spyware/Malware Detection
- Network Breach Detection
- Digital Debugging
- IT Network Vulnerability Assessments
- Background Investigations
- Under Cover Work
- Surveillance
- Corporate Intelligence
- E-Discovery

Digital Spying and Cyber Stalking in Divorce

Divorces can often become so contentious that warring spouses will go to any means to gain the upper-hand in the settlement. Spyware and key loggers that

used to be only available to governments and corporations are now inexpensive and easily accessible to even the most novice computer user. Not only are monitoring applications more prevalent, GPS and physical listening devices are available for amateur spies. Emails, text messages and images as well as social media sites such as Facebook and Twitter are becoming key sources of evidence in divorce cases. The installation of spyware and key loggers is becoming more and more common, a real possibility and no longer in the realm of the paranoid or crazy.

Spying on a spouse is not limited to only monitoring of computers and mobile devices. With advancements in technology, GPS tracking is more readily available and is no longer cost prohibitive to the average person. Technology now allows for real-time tracking from any computer or smart phone with an internet connection. At around $150.00 (plus the monthly service fee of around $30.00), the match-boxed sized devices can be hidden in a bag or inside a car. The devices can also be attached to an extended battery and a weatherproof magnetic case and attached underneath a vehicle. Community property laws in some states do not prohibit the GPS tracking of a vehicle given that both spouses can have an interest in the vehicle.

Tracking location is not limited to GPS devices. Even smart phones have location applications available. A spouse can purchase an additional iPhone or Android-based device on the same account, turn on the location feature, hide the phone in a car or bag and use another phone or a computer to track the location of the phone. With the hidden phone being unused, the battery will often hold a charge for 24 – 48 hours allowing the spying spouse to see in real time where the device is located.

Physical listening devices and video cameras are also easily available and relatively inexpensive. Cameras and listening devices can be disguised as teddy bears, house plants, cleaning products, garden stones and other common household items. Or the devices can be small enough to be hidden anywhere within the home or office without being easily discovered. These items can be purchased from any internet spy shop, often with extended battery life and memory cards ensuring that the video or audio can be recorded for long periods of time. Physical listening devices can violate federal wiretap laws, however, the interpretation of the law varies from state to state. In some cases, the federal wiretap laws do not apply to “interspousal wiretaps”, however in another state, a spouse may be charged with federal wiretapping for utilizing a listening device to spy on a spouse. The laws clearly have not caught up with the technology.

Technology has made cyber stalking even easier and more dangerous and frightening. Spousal spying can easily become cyber stalking, especially if the spouse threatening or violent. It is much easier to stalk a victim, even if it is a spouse, by utilizing technology to gain knowledge of the whereabouts through GPS location, their financials and private personal affairs. This can not only endanger the victim, but anyone who texts or emails them as well as they are brought into the cyber stalkers circle.

Client Situation

McCann Investigations was presented with a case in which the client was involved in a high net worth divorce case and believed that her spouse had bugged her computer and possibly her mobile device in an effort to gain information in the divorce settlement. The client, who was fairly wealthy believed that the spouse was bugging her electronic devices in an effort to gain not only

information about her bank accounts, but also to spy on her personal affairs to gain knowledge on her friends and whether or not she was dating.

While gathering the case background, the client shared that she believed she was the victim of a predatory con-artist who had taken advantage of her vulnerability after the death of her husband of 40 years, a wealthy businessman. She believed that she was manipulated by a man who was clearly after her money, and had made the mistake of marrying him. She suspected that the man had installed spyware on her laptop and computers in order to gain information about her financials. Upon filing for divorce, the client feared that her husband was able to access her accounts and that he may have also installed listening devices in her home as he had information about her that he could not possibly have had any knowledge of. She became even more suspicious when she discovered that she was inexplicably locked-out of her email accounts as well as her Facebook account. The passwords had been changed, but she did not change any of the passwords herself.

The client also shared that she felt that her husband was stalking her as he would often appear at the same event, restaurant or store that she was at when she had never given him any information about her whereabouts. She would even see his car drive by when she was visiting the homes of her children and friends. She again saw him watching her from his car on an evening walk in the neighborhood park. Again, she never gave him any indication of where she would be at that time.

Suspicious that she was the victim of spyware and cyber stalking and given that she was in the midst of a divorce in which a large sum of money and assets were at stake, she contacted McCann Investigations. McCann Investigators were

contracted to forensically examine her computers and phones as well as perform TSCM (Technical Security Counter Measures) investigation on her home.

Technical Situation

The client had one laptop and one computer at her home which she suspected were bugged. She also had an iPhone 4S which she also thought may have spyware installed as her spouse had access to all of her computers and phone when they lived together. While spyware can be installed remotely on a computer if the perpetrator is tech savvy enough, spyware must be physically installed onto a smart phone.

There are no tools that can detect spyware on an iPhone at this time. The only way to determine whether or not spyware has been installed is through "symptoms" in the iPhone's functions. These symptoms can include:

- Lack of responsiveness. Because the spyware runs constantly, it causes other applications to run slowly as well. Or the device may not shut down easily or may remain lit for a few seconds after shut down.
- Excessive battery drain. The constant running of the spyware as it gathers information and sends that information "home" will drain battery even when phone is not in use.
- Increased phone bill. The continual transfer of data over the internet can cause data overages if the phone does not have an unlimited plan.
- Increased internet activity. An iPhone has a small icon on the top left of the screen that indicates when data is being transferred through the internet. If this icon is active, when the user is clearly not accessing the internet, it could indicate the presence of spyware.

- The GPS location icon appears to activate, indicating that the phone location is being tracked.

The client reported symptoms on her iPhone 4S which indicated that she most likely had spyware installed. She had indicated that shortly after her husband moved out, her iPhone began to run very slow in every application. She also indicated that her iPhone would often inexplicably vibrate or tone when she was not touching it. Her battery also began losing its charge in a very short time period. For example, if her phone was fully charged at night when she went to bed, she would wake up in the morning and the phone would be dead. She often noticed that the phone appeared to be accessing the internet, even when she was not utilizing any applications that may require internet use.

McCann
INVESTIGATIONS
Information | Insight | Influence

Solutions

McCann computer forensics examiners ran spyware detection (Mandiant Redline) applications on the client's computer and laptop. The examination determined that there was a key logger and spyware installed on the devices. McCann investigators removed the spyware and installed software to detect future spyware and key logger installation. McCann Investigators recommended that the client purchase new computers as well as a new router.

Because there are no tools to detect and remove spyware from an iPhone, the only way to remove the spyware is to factory reset the phone. Basic information such as contacts and photos can be backed up to iTunes. It is important not to back up the applications, as this might inadvertently reinstall the spyware. The iPhone can then be restored without the applications. However, in order to be sure that there was no spyware on the phone. McCann recommended that the client replace her iPhone with a new one.

McCann Investigators also checked the client's vehicle for GPS devices. In addition, Mcann also performed a bug sweep (TSCM) in the client's home and did not find any listening devices. No GPS or listening devices were found on the vehicle or in the home.

Products and Services Used:

- Computer Forensics Technician – Licensed Private Investigator in the State of Texas with certification in computer forensics.
- Mandiant Redline – Leading spyware detection and removal software

- EnCase, a Guidance Software – Leading software application to forensically image computers.
- Oxygen Forensic Suite – Leading software application to forensically image Smartphones.

Conclusion:

With the pervasiveness of technology in modern life, spying spouses with very novice technology background have access to tools that are inexpensive and easy to install. Even utilizing physical listening devices (bugs) and hidden video cameras, a tactic long used in corporate or international espionage is available to the general public. Spying can allow a husband or wife to gain the upper hand in a contentious divorce where there are significant assets on the line or complex child custody issues. Because laws have not caught up with technology, there can be a gray area in privacy issues when it comes to married individuals.

A highly complex and sophisticated divorce is a stressful, life-altering event. It is important that the victim understand what counter measures can be implemented to protect sensitive information on computers, laptops and smart phones as well as to protect their privacy from spying spouse.