DOWNLOAD PDF INTERNET INVESTIGATIONS IN ELECTRONICS

Chapter 1 : Cyber Crime Investigations - Law Enforcement Cyber Center

Note: Citations are based on reference standards. However, formatting rules can vary widely between applications and fields of interest or study. The specific requirements or preferences of your reviewing publisher, classroom teacher, institution or organization should be applied.

Electronic Surveillance What is electronic surveillance? Electronic surveillance is the monitoring of a home, business, or individual using a variety of devices such as CCTV, legal wiretapping, cameras, digital video equipment, and other electronic, digital, and audio-visual means. Today, electronic surveillance can also refer to surveillance done via computer or mobile phone. For example, computer surveillance can include e-mail tracking, internet surveillance, and remote PC surveillance. Why use electronic surveillance? If you want to keep your home safe, electronic surveillance can monitor what is happening in your home even while you are away. The same applies to a place of business. A combination of video and audio surveillance gives you the most complete picture of what is happening at a specific place and time. It is a way to oversee behavior, activity, and information for the purpose of protecting, managing, or influencing a certain location. Is electronic surveillance legal? In many states, there are laws that stipulate who can use surveillance techniques and how they can use them visit our page on audio surveillance to learn these laws by state. Electronic surveillance laws are especially strict because there are many ways that it can be used to invade privacy. For this reason, it is imperative you never attempt electronic surveillance yourself. Not only will any findings be potentially inadmissible in court, but you may find yourself facing a lawsuit. A trained investigator has experience with electronic surveillance and knows the laws surrounding it. Computer and Moblie Phone Surveillance Information found on computers, tablets, and mobile devices can be valuable when conducting an investigation. Failure to monitor a computer can result in crashes, lost data, or stolen information. Electronic surveillance can alleviate or eliminate fears business owners have regarding computer security. Mobile Phone Surveillance Electronic surveillance of mobile phones is quickly becoming a viable means of gathering information about an individual. Geographical location can be fairly easy to track and is helpful when determining where an individual will be in the future. More often, text messages and phone records are being used as evidence in court. For example, inappropriate phone interactions can be an integral part of an infidelity investigation. Am I under electronic surveillance? If you leave your home, you are probably under some form of surveillance. Many banks, businesses, and companies use electronic surveillance to monitor activities and have footage in the event of unlawful activities. Cities are following suit by installing cameras and other digital monitoring devices in public places. Do I need an electronic surveillance investigation? If you want a better security system for your home or business, electronic surveillance may be your best choice. Electronic surveillance systems are a practical means for securing your home or business. Having the facts on video, in photographs, or in another audio-visual format can give you the factual information you need to win a case. What can I expect from an investigator specializing in electronic surveillance? If you are concerned about the safety of your business or home, an investigator trained in electronic surveillance will analyze and record any suspicious or criminal activity. They do this by discreetly following a subject or setting up cameras to document their activity. An investigator will be licensed in the state they are serving, have equipment that properly records details, explain to you their surveillance plan, and be an expert witness in the event they need to testify in court.

Chapter 2 : Concord business owner charged in electronic gambling investigation

"Internet Investigations" meets the needs of professors, students and others interested in learning how to use the Internet in career fields. This cutting-edge guide provides step-by-step, easy-to-follow practical information to help you begin using the Internet for finding valuable information.

In short, if a device is able to connect to the internet, it can probably be used in electronic surveillance practices. Different countries have different laws, so obviously the legality of electronic surveillance varies by country. With the technological advancements of the last few decades, however, governments are introducing new laws to increase their collection capabilities. Surveillance is legal under certain circumstances, but many critics of surveillance laws point at the indiscriminate nature of many of the measures taken. As a result of this, the legality of many surveillance practices has been challenged in court, with varying results. Some courts have upheld surveillance laws while others have put a halt to certain aspects of electronic monitoring. What is an IMSI-catcher? IMSI-catchers are devices that can be used to listen in on mobile phones without the either of the callers knowing. The tool poses as a fake mobile phone tower, which means mobile phones send all information that would usually be sent to a regular tower through this device. That means that innocent bystanders have their privacy invaded. Since the technology used in IMSI-catchers keeps progressing, these devices are getting smaller and smaller. They can now be mounted on small drones. Even body-worn IMSI-catchers are being sold. What is an IP-intercept System? IP-intercept systems like the one shown in the Al Jazeera Investigation, are used to collect internet traffic for large groups. The system records which computer or phone visits which website and, in certain cases, see what the user is doing on this site. This makes it easy for governments to monitor citizens, to see, for example, if they are posting things that could be conceived as illegal or inflammatory. IP-intercept systems are a good way for oppressive regimes to follow what their citizens are doing online. These tools have been used to quell resistance movements in, among others, Egypt and Syria. By following members of the opposition on the internet, law enforcement agencies were able to track them and arrest them. I ha ve nothing to hide, so why should I care? Everybody has things they want to keep private. It might not be anything illegal, but everyone has certain elements of life that he or she would rather not put out there in the world. When someone is suspected of having committed a crime, authorities could go back to any conversation ever held and use this against the suspect, even though it might not have anything to do with the crime in question. Journalists will have a harder time doing their jobs because stories often rely on sources that do not want their information made public. It becomes a lot harder for people who want to leak criminal or dubious practices by governments or companies to safely to do this when all communication is being monitored. And, as the earlier mentioned examples of Egypt and Syria show, there are legitimate reasons for wanting privacy when communicating with other people. Fear of speaking out helps oppressive regimes strengthen their grasp on their citizens. How can I make sure my communication remains private? There are several ways of making sure your communication is not being read or seen by anyone. One of the most important aspects of this is encryption. If you want to send text messages, use Signal or WhatsApp since they use end-to-end encryption. This means only you and the person you are texting with can see the messages you send and receive. There are other apps, like Telegram, that use different encryption models, with varying results. But even these are not completely safe. A recent disclosure by WikiLeaks shows that agencies like the CIA are very adept at finding ways to get the data they need. Internet websites have increasingly been switching to so-called https-connections, which means that any communication between the website visitor and website owner remains private. This is especially important when dealing with sensitive information, for example, when putting in credit card information or filling in tax forms online. These secure https-connections can be recognised by the green lock in the address bar of the internet browser. A VPN service puts all internet traffic through a private tunnel, which increases privacy and makes it harder for anyone to snoop on what you are doing on the internet. This is especially important when using public networks in, for example, airports or coffee shops. Even safer is using a service called Tor , that completely obfuscates your browsing by sending your internet traffic through several locations in the world. Setting this

up is a bit more complicated, but for people that need privacy the most - mostly those living under oppressive regimes - Tor has been a lifesaver, in many cases literally. Another important aspect is password security. It is important to use different login specifics for different services, and all of these passwords should be hard to guess. These services act as a safe for all your passwords, so it is important to never forget your so-called master password to access your vault which stores all your other passwords. Adding to password security is turning on something called two-factor authentication for services that support it. This creates an extra layer of security when logging into services like Gmail, iCloud or Amazon. Even when someone has somehow obtained the password, it will be useless because they need a randomly generated code that is created by the two-factor authentication. A good comparison is having a door with several locks: Lastly, there are some common-sense solutions, as well. Complete security is almost impossible, especially when confronting nation-states and big intelligence agencies that have a lot of resources, both financially, as well as in personnel. These precautions, however, will serve as an extra layer of protection against any malevolent actors that might be using electronic surveillance. Besides that, having taken these precautions will also serve as a protection against certain types of cybercrime. A lot of personal information is stored online these days, so it makes sense to ensure this information is kept safe. Who sells surveillance systems? There is a thriving private intelligence industry, both in the public and private sectors. A lot of different corporations and governments create hardware and software that then will be sold to the highest bidder. Who buys surveillance systems? Both governments and private parties buy surveillance systems, but governments remain the biggest buyer. They have the resources to acquire these kinds of systems and get the most use out of them. There are legitimate uses for these kinds of surveillance systems, as they are often used in regular criminal investigations, for example. Attacks in several countries that have some of the most powerful intelligence agencies in the world have taken place despite the fact that these attackers were under surveillance. There are several reasons for this. First off, as mentioned, at this moment there are still ways of communicating privately without it being monitored. Second, when conducting mass surveillance, it is really hard to find that one needle in the haystack to prevent an attack. This is especially true now that huge amounts of data are being collected. Targeted surveillance has often proven more effective than collecting everything and sifting through all of the data. Attackers, however, only need to be lucky once to successfully conduct an attack. Monday, April 10 -

Chapter 3 : Digital Forensic Services-Cyber Investigation Services, LLC-Internet Investigations

Find helpful customer reviews and review ratings for Internet Investigations in Electronic Technology at calendrierdelascience.com Read honest and unbiased product reviews from our users.

Chapter 4 : Electronic Surveillance Investigations - calendrierdelascience.com

Internet based If the case is internet based, finding the internet protocol (IP) addresses is your first step in the investigation. An IP address consists of numbers and letter, and that series is attached to any data moving through the internet.

Chapter 5 : Spy Merchants: What is electronic surveillance? | Spy Merchants | Al Jazeera

Electronic surveillance is the monitoring of a home, business, or individual using a variety of devices such as CCTV, legal wiretapping, cameras, digital video equipment, and other electronic, digital, and audio-visual means.

Chapter 6 : Internet Crime Complaint Center (IC3) | Home

The Internet Investigations Training Program (IITP) is designed to give investigators, analysts, and individuals serving as direct law enforcement support a basic understanding of and the skills needed to conduct Internet-based investigations.

Chapter 7 : Training - Law Enforcement Cyber Center

About Forensicon, Inc. Specializing in trade secrets, employment litigation, and internal investigations, Forensicon is a computer forensics firm that provides expertise to the top law firms in the U.S. as well as corporations large and small.

Chapter 8 : Internet Private Investigations | Cyber Investigator | Monitoring

It is recognized that all investigations are unique and the judgment of investigators should be given deference in the implementation of this special report. Circumstances of.

Chapter 9 : - Internet Investigations in Electronic Technology by Cynthia B. Leshin

for electronic crime. Unlawful activity can be committed or facilitated online. Internet Investigations Training Programs Financial Fraud Institute.