Stalking by a “High Tech” Guy

A View from the Other Side

By John Loveall

2005

Table of Contents

Introduction

I could be called a “high tech” guy – I’m “into” technology, put my own computers together, and work in the computer industry. I take some pride about being informed about technology and friends often use me a “tech” resource for questions. I’m not a trained private investigator, nor do I own a collection of “stalking” gadgets. Let’s just assume that I am resourceful, learn fast, and know how to use most any technology just by picking it up and trying it. And one more thing: When I don’t know something I’m really good at finding information on the internet.

Given that background, it’s interesting to ask what a guy like me would/could do if I wanted to do either of:

1. Stalk you if I didn’t know where you were
2. Stalk you if I did know where you were

If the goal is to stalk you, then it’s certainly interesting to know where you are. I’ll talk first about how I would go about finding you, and then go from there to what I would do once I knew where you were. I’ll also assume that the reason why I want to stalk you doesn’t affect what I would do until I know where you are.

Finding You

Before I talk about what I would personally do to find you, I want to mention the obvious alternative: hiring someone to do this for me. While actually stalking you once I know where you are can be a much more

personal activity, the job of finding you can be fairly mechanical and is what private investigators (PI's) do for a living. If I have some money to spend, I could easily use the web to learn how to choose a good PI and then search for one I like. This is really easy, although somewhat traceable.

Also, it's important to realize that, depending on how much you don't want me to find you, you could also follow the steps I would take to see how "findable" you are. Do the steps I list yourself and see what I will know about you. Remember that it gives me power to know more than you, so you might want to take a little time to educate yourself. After all, I'll be spending a lot of time doing just that.

The remainder of this section will assume that I've decided to find you on my own.

Step 1: What do I know?

The search starts by knowing something about you. The more I know, the more ways there are to try to track you down. Let's assume that I have a basic set of facts:

- Your name, or at least what your name was at some point (you may be using an alias now)
- Your occupation, or at least what you did at some point in the past
- Your approximate age
- A picture of you, from some point in the past

Those are fairly basic facts. Depending on my previous relationship with you, it is likely that I would know any number of other facts about you, like:

- Where you lived
- Family: names, relationships, locations
- Friends: names, locations
- Where you went to school and what you studied
- What general job skills you have
- What email, on-line names or aliases, or passwords you have used or prefer
- What kind of computer you have, what the system name is, etc.
- What kind of cell phone you have
- Your preferences in:
    - Places to live
    - Restaurants
    - Places to go on vacation
    - Stores
    - Clothing
    - Movies
    - Music – e.g. bands
    - Cars
    - Hobbies

It's amazing how much information you can gather about people you know if you stop and think about it. Of course, being resourceful, I would also go on the web and search for information on private investigator methods. Googling on such phrases as "private investigator questions" or "private investigator interview" will pull up web pages, books, and even correspondence courses I can look at to see what other kind of information PIs find useful.

Step 2: Look for a Trail

Once I have my facts, the next step to finding you is picking up your trail. Once I know at least a recent place you have been, I can dig in and look for more clues from there. Think of how a blood hound works: once he has your scent he looks for it somewhere to pick up the trail. In our case, your “scent” is the information I know about you and the “trail” is any place (more recent the better) that I can find where you have been.

My first inclination is to see if you’ve left an obvious trail and use the web to search on your name. This can turn up any number of common on-line references:

- Phone listings
- Resume postings
- Newspaper articles
- Committee minutes
- Author/artist credits
- Logged email or chat room sessions
- Your personal web site

A hit anywhere and I can dig further, either on your information or on someone else’s that is listed with your name that might know something.

Not forgetting “low tech” approaches, a great way to find you is to just ask someone else who knows. This is where names of other people that know you, like family, friends, and co-workers become very useful. Also, addresses of places where you lived or worked can be help to make contact with others who may know something. Or if I suspect you are in town but hiding, I could start spending some spare time at places I know you like to go, just to watch for you.

I’ll assume the case where you know me and have been smart enough to tell some people that I might be looking for you. This means that I will want to hide who I am when asking for your location. Phone calls and email to people are my next choice, using any number of ploys. Phone calls claiming an important package for delivery, an important automobile recall notice, a final paycheck to deliver, or escalating collection issues for a bill not paid are all easy ways to anonymously get someone to tell me how to find you. Of course, in the on-line world, if you know people’s email addresses, it’s easy to craft “spoof” emails claiming similar things and in email it’s easy to put in company logos and official-looking links to company web sites to appear more legitimate than a voice on the phone might be.

You can see why, if you’re smart and want to hide from me, you’ll get the word out to all of your family and friends to be on the lookout for contacts either from me or from anyone that claims to be looking for you. You should ask them to never respond to any of these inquiries and instead just let you know if such an attempt is made.

If these efforts fail, the next step I would take is to spend a little money and subscribe to one of the “super search” web services. These sites (the same ones that I would subscribe to if I looked for people for a living, or that direct marketing people use to create their mailing lists) provide access to the growing amount of on-line public record information. This includes court records (e.g. traffic tickets, foreclosures, evictions), real estate title transactions, and any number of databases that can be used to find you. The nice part about these services is that I can gain access to them 24 hours a day from the privacy of my own web connection, for a few 10’s of dollars on a credit card.

Example “super search” sites:

- http://find.intelius.com/
- http://www.peoplefinders.com/
- http://www.aaronspi.com/
- http://www.phonelosers.org/pi.html

Step 3: Follow the Trail to You

Once I have a "hit" on your trail, I'll just follow the clues to the next steps you took. Each "hit" can provide me with more information, e.g. addresses, names, email addresses, companies, that I can then leverage to find the next step.

The trail can either lead to you physically, e.g. your current address, current place of employment, current school, or it could lead to one of your "on-line" locations, e.g. an email address, chat room alias, or EBay merchant name.

If I had an "on-line" location, next steps I would take to follow your trail are:

- **Email address**: If I had what I thought was your email address, I have a few options. If I'm lucky and it's a work address, then I just need to look up the company's website, put in a call to the HR department acting like a company that you interviewed with and then verifying your employment status. If it's a personal email address I would send a "phishing" email to try to get you to tell me your location or if nothing else to get a response email from you so I could look at the email headers.
    - **Phishing email**: I'd send a phishing email notifying you about something important that needs you to go to a web site and enter some information. The more I know about you, .e.g. where you shop, what restaurants you go to, where you went to school, the easier it is for me to avoid raising your suspicions. For example, if I know where you went to college, I could send an email, complete with the college logo, real links to their website, and current names of administrators, stating that there is a new program for alumni to receive, free of course, a new quarterly journal along with opportunities for great on-line discounts previously only available to their faculty but now, through a gracious agreement with the college, is now open to alumni. Example would be televisions at 55% discount, travel at 60% discounts, and automobiles at an amazing 70 to 75% discount. The list would of course be tailored to your tastes. And of course the web site you go to from the link in the email would look just like the current style of the college website, and it would ask for your name, graduating year, current address, and, optionally, some information for their records like current occupation and other advanced degrees. Of course, the web page would live on my web site, and the information you type would tell me just where to find you.
    - **Email headers**: In the case of the spoof email, a fallback plan would be that you replied to the email telling me to take you off my mailing list, so some such thing. I don't care what you type – I just want to see the email headers in your email. These let me know:
        - **IP addresses**: The internet addresses of your computer and internet service provider. This minimally gives me something else to key a web search on, where no matter what email aliases you were using, I can find emails or other postings originating from your home system. And of course more information for more next steps. I would also take all the IP addresses and decode them at a website like http://www.dnsstuff.com/ or http://remote.12dt.com/rns/ to see what it tells me about the service provider you're using. I'd also try to send phishing email to the internet service provider to try to get your account information. I could also send you more phishing email appearing to come from your internet service provider, perhaps complaining about an unpaid bill and with a link to update your current account information.
        - **Email software**: The headers often contain the name of the software you use to send your email, e.g. Microsoft Outlook, Outlook Express, or Mozilla. I can now think of another phishing email to send you with important information about, say, new security vulnerabilities found in your specific email software, asking you to provide some information to receive more information and an update…
        - **It's you**: Of course, getting a response of any kind gives me another chance to verify that I have a good email address for you and that I should keep trying. And

maybe your email contains a cute signature appendix that has more information, or a nice graphic that has web site information embedded in the HTML in the mail message that I can find…

- **Chat Room Alias**: I’d join the chat room, read as many of the existing logs of previous chats that you participated in, and when I saw you were on-line, I’d use my personal knowledge of you along with anything I learned from reading the chat logs to get you to interact. I’d then just try to get you to tell me some new facts about where you lived, worked, went to school, shopped, went on vacation, etc. Anything you tell me adds to my database and gives me ways to take next steps down the trail to you.

It’s interesting to note my personality and how it affects my search for you. Remember, each new lead I get will reward me and give me more energy to find the next one. As a “high tech” guy I take it as a personal challenge to solve this problem, using any and all tools I can find. I’ll be thinking that I’m smarter and better at this than you are and it will really bother me if I can’t find you. Finding leads to you will provide me ongoing reinforcement that I’m a smart guy and you’re not. I’ll be thinking about how to find you when I get up, on my commute, at work, at lunch, and at night. I have access to the web at work and at home, so I’ll be able to search and email constantly. I’ll use my home system to set up some automated searches just in case something new about you shows up. Eventually, if you have any presence on-line at all, I’ll find it and use the information to take the next step down the trail to you.

Stalking You Now That I’ve Found You

Once I’ve followed your trail and found you, the “personal” phase of the stalking can begin. By finding you, I mean that I now know a way to reliably know where you physically are. This can mean address where you go on a regular basis, e.g. home, work, school, store, gym, church, friend’s home, bar, nightclub, etc. By “personal”, I mean that what I now do with this information, and how I try to stalk you, depends on my motivation for stalking you in the first place.

What I Do Depends on Why I’m Doing It

The techniques I’ll choose to stalk you depend on what I’m trying to accomplish. The basic goals I can think of for stalking you fall into a few categories:

- **Date you (get you to like me and want to be with me)**: In this case, I want to have chances to “meet” you for the opportunity to convince you, somehow, that you like me (or whoever I’m pretending to be in disguise) and want to spend more time with me.
- **Scare or hurt you:** I want to intimidate, scare, damage, or even kill you. Note that this means that I’m potentially not just interested in you, but also in people or things that are important to you.
- **Have a vicarious relationship:** I don’t hope (perhaps yet) to have an actual relationship with you, but if I eat at restaurants you like, see the movies you see, shop at stores you shop at, read books you read, take classes you take, take vacations where you take vacations, etc. I can pretend that we are getting closer and closer with each passing day.
- **Voyeurism:** I want to watch you, whenever I can, whatever you are doing. I am obsessed with knowing where you are, what you are doing, what you are wearing, who you are seeing. I want to see you every chance I can get, whenever I want.

What Technology Helps Me Do

Once I’ve understood the goal I have for stalking you, I have a general set of tools to choose from that help me do the job. These tools have three basic uses of interest to me:

Technology That Lets Me Know You're Nearby

These tools are useful to discover your presence in an area. Some of them are also useful to do more advanced things (see below), but it's important to realize that in their simplest and easiest use, they can tell me that you are nearby. (And sometimes that's all the information I need.)

- **Location**
    - **GPS**: Global Positioning System (GPS) receivers are small enough to secretly attach to your car. Various connectivity schemes exist, including connection of the device via HAM radio. The interesting thing about HAM radio connections is that they are low power and, due to the use of HAM radio for emergency communication systems, they have receivers everywhere, even in fairly remote areas. It's straightforward to track your location on a live web page as a marker on a map.
    - **WiFi**: If you use a laptop with WiFi (802.11a/b/g) wireless capability and I know your system name, I can listen for your broadcast signal and detect that you are within a few hundred meter radius of where I am sitting. I can scan for you by driving by your house or outside the walls of your office.
    - **Bluetooth**: If you use a laptop, mobile phone, or PDA with Bluetooth wireless capability, there is a reasonable chance that you have not changed the default security settings and, if I know your system name or type, I can listen for your signal and know that you are less than about 50 to 100m from me.
    - **IR**: Most laptops and many PDAs have an infrared communication port on them. I have to be in a line of sight with you, but if you have left your port open and I know the name of your system I can take a handheld PDA and scan a small group of people and detect you. This is more inconvenient, and I'd rather detect you with the longer range WiFi or Bluetooth technologies.
    - **RFID**: This is mostly useful in the near future (2005 and later) as RFID technology replaces the UPC code on all products we buy and reader equipment becomes inexpensive. It provides an ability to detect you if you if you are carrying or are wearing any items that continue to have their RFID tags attached. It's also useful for providing a way to track items that I attach an RFID tag to, such as your car. If I place a tiny RFID tag on your car and place a small RFID detector by your garage door, using various connection technologies (including cell phone calls and HAM radio transmissions) I can detect if you have just pulled your car into or out of your garage. This can be a little easier than planting a GPS receiver on your car, since RFID tags can be as small as grains of sand, and I can take more time planting the reader on the outside of your house when your are not there.
- **Visual Detection**
    - **Web cam**: While web cams are usually associated with watching live video, they can also be connected to a computer running motion detection software. I can plant a web cam watching your garage, front, or back door and have a computer looking for motion that can call or page me upon detection, including sending me a still photo of what it just saw. This gives me a way to know where you are without watching a video feed all day (after all, I'm a busy guy…).

Technology That Lets Me Intercept Information from You

The next step up from detecting your location is to get information from you. This information could be what you're typing (e.g. email, web sites, passwords), what you're saying (e.g. cell phones), or what you are doing (e.g. web cams).

- **Spyware**: If I can get access to your computer system, I can place spyware on it to read your every keystroke, allowing me to not only spy on everything where you go and everything you say on-line,

but also to hear all your login and password information. This is why you need to firewall and virus-protect your system and not install software with which you aren't completely familiar. It's also why it's important to physically protect your system including boot password protection, so I can't break into your home, fake a robbery as a diversion, and load spyware on your system that you likely won't even think about checking since you'll be so grateful I didn't steal your computer.

- **WiFi**: If you're not encrypting the data in your wireless networking connection, I can set up a receiver and read everything you send over the network. I may not be able to easily read your passwords and sensitive information since most web pages use separate encryption for that data (a good reason to check for a secure page, e.g. the small yellow lock icon in Internet Explorer, before you enter sensitive information on a web page.)
- **Bluetooth**: Like for WiFi, if you have not enabled encryption in your Bluetooth connection, I can read all the data being transmitted.
- **Cell / wireless phones**: This is a bit harder to do and requires more expensive equipment, but it's possible to listen to anything you transmit. This is why people still recommend switching to a "land line" for sensitive conversations. I can still tap your land line, but that will probably require me to at least enter your backyard which is riskier than listening in my car down the street. (However, people often don't realize how exposed the phone lines are when they enter your home. A few dollars at the local Radio Shack gets me the tools needed to splice into your phone line.)
- **Web cam**: I can either plant a web cam outside or inside your house or I can set up a receiver for any web cams that you have placed around your house. And don't forget that these tiny cameras can look into your windows if I don't want to actually break in.

Technology That Lets Me Interact With You

Knowing your location and watching you is great, but eventually I'm going to want to actually interact with you. For high tech tools, this means sending you computer data (e.g. email, digital media, software), talking to you (e.g. phone calls), scaring you (e.g. causing sounds or commotion where you are), or even hurting you (e.g. remotely exploding a bomb).

- **Email**: Once I have your email address, sending you email is the easiest way to interact with you. If nothing else, I know that unless you have learned to filter me out, each email I send will cause you to react. That's a very powerful feeling. (Something for you to remember is to not immediately destroy an email address as a response to me. If you do that, my email will start to bounce, and I'll know you're not getting it.) However, I can do several more things with email to you.
    - **Phishing email**: Since I have found you, I don't need to lure you to a web site to get your address or phone number. However, I can still send these emails to extract information such as credit card or bank account numbers. I can also make you worry by sending you alarming notices, e.g. credit problems, lawsuits, bench warrants from unpaid traffic citations, communicable disease notices due to a friend's diagnosis, etc.
    - **Email signups**: With an active email, and possibly your address and phone number, I can start signing you up on all kinds of lists, e.g. pornography, white supremacists, etc.
    - **Spyware email**: I can bundle spyware with my emails and try to get you to install it for me on your computer. These emails can be disguised and can be tricky, such as making the link to "remove from our mailing list" be the button to install my software. Your anti-virus software may stop me, but I don't have much to lose by trying.
- **Chat**: If you chat and I know your identity, I can pretend to be anyone I want and interact with you. This can be for fun, to fool you into doing something, or to disturb you whenever I see you on-line.
- **WiFi**: If your home wireless network is not password protected, I can log into your network and search for shared disk drives or printers. If there are unprotected shared disks, I can put anything on your disk I want. If I find a shared printer, I can print anything I want inside your home.
- **Bluetooth**: If your Bluetooth device is unprotected, I can try to access whatever Bluetooth device I can find, e.g. printers, PDAs, laptops.
- **IR**: If you're IR port is not protected, I can carefully get close to your computer and send you files. This is not as intrusive as directly accessing your disk, but it can let you know I've been there.

- **Actuators**: The advent of the “smart home” has provided a completely stocked playground for people like me. The same technology that allows my home computer to switch lights on and off through wireless modules or through the power lines also allows me to install remote devices that I can activate from my computer. For example, many houses today have outside power sockets. If you don’t switch these off, I can connect a smart home module and receiver that I can activate from my laptop from the comfort of my car just down the street. This device could do anything from making noise in the middle of the night to exploding into flames, just as easy examples. Now imagine what I could do if I planted these devices inside your house.

Putting It All Together – Stalking You

Put the goals for stalking together with the tools and I can work on a number of scenarios for you. These are short examples of what I can do depending on what I know about you, what stalking vulnerabilities you have, and the goal I have for stalking you.

Stalking Example 1: Stalking to make you like me

In this case I want to get mindshare with you which can either be an online anonymous contact (in the case where you know me and won’t interact) or an in-person meeting.

In the online case where I need to hide my identity, I would want to track down your email, which will be interesting for awhile if you respond to me, and then eventually move to a live chat session to we could “talk”. I would of course make up a different identity, but I would likely only change obvious things like my name. After all, if you won’t interact with me if you know who I am, I probably want to “prove” to you that you’re not being fair by showing, eventually when I choose to reveal it to you, that you like me on-line with a different name. This is like the “pina colada” song scenario, except I know it’s really me and you all along.

If I’m actually a stranger or someone that you have ignored in the past but want to convince you to like me, I would want to create as many “coincidence” meetings as I could to allow me to interact with you. In this case, I would want to track you continuously to understand your daily routine and so a GPS receiver attached to your car would be great. The problem is that I want to avoid actually following you everywhere, but I need to know where you’ll be to “meet” you. So finally I would want to narrow down the locations to meet you to particular stores, restaurants, etc. meaning that while the GPS might go be good enough, if you’re, say, arked at the mall I may use my handheld PDA to look for your PDA’s or mobile phone’s WiFi or Bluetooth signal. Of course, when we do meet, I’ll use all of the other information I’ve gained from web searching, spyware, or phone tapping to lure you into a conversation with me. Note that without even tracking you I can use my on-line information to find out meetings or other scheduled time you have corresponded to other about and arrange to be there.

Stalking Example 2: Stalking to hurt you

I can hurt you by affecting you emotionally or physically, and I can affect you directly or by affecting people or things dear to you. If I mainly want to annoy or punish you, then I can use any of my on-line connections to make your on-line life unlivable. I can use email or on-line identities you have to flood you with contacts, both from myself as well as by subscribing you to mailings from others. I can set up automated searches for email addresses that may be associated with you and then put those on a list that I feed to other automated programs to flood them. I can also do the same thing to your friends and colleagues if I can get their addresses, embarrassing you as well as hurting them.

To physically hurt you, I can either work to set up something remotely to hurt you or arrange to meet you where I can hurt you directly. For example, it’s easy to set up incendiary devices to be remotely activated. I can buy model rocket engines with remote electric starters, mount these in gas cans and hook up a remotely controlled “smart home” light switch controlled by my laptop from my car. In other words I can create a powerful, remotely controlled bomb with a few purchases at my local shopping mall. I could use the GPS I

placed in your car or a remote web cam with motion detection software or, more likely in the future, an RFID tag and sensor to determine when you’re home, or even in the garage if I want to be more precise. I could even place an inexpensive remote computer to trigger this for me, but I would probably want to monitor this personally since I don’t want to hurt anyone accidentally and there is s certain amount of satisfaction to pushing the button myself.

And of course I can do all these things to people that you care about as well.

Stalking Example 3: Stalking to have a vicarious relationship with you

To mirror your activities, purchases, and overall lifestyle, I mainly need to be able to watch you closely. Location isn’t good enough for this – I really want to be able to see you. I can do this personally by following you with my laptop web page tracking a GPS receiver, for example, but I’d rather be able to watch video remotely if I can. In either case, web cams with motion detection software are great ways to detect and monitor you at known locations that you frequent. I can also get a lot of information from you by sending you phishing email asking for extensive personal information. Imagine what you’ll tell me, for example, to get a free TV for answering a marketing survey about your opinions of various styles from Victoria Secret’s new catalogue.

Stalking Example 4: Stalking as a voyeur

As a voyeur, I mainly want to see you in ways others can’t see you. I want a special seat, just for me, that lets me see you in your most private moments or doing things in situations that I contrive. The key is that it’s a special view, unique to me. Note that this “view” can be your data in addition to your video image. Reading or listening to your intimate communications satisfies my need for a unique, private view as well as a web cam in your bedroom (or bedroom window) might. This means spyware and phone taps are as interesting to me as a web cam, and in some cases perhaps more interesting since your communications can tell me your intimate thoughts. The tricky thing for you is to detect me – since my overall goal is to have a private seat I don’t want to alert you to my presence. If I do my job correctly, you won’t ever know. This means that if you don’t want me to watch, you will have to take pro-active steps to keep me away and can’t simply wait to react to a “problem” that you see.

The Bottom Line

Technology is a dual-edged sword. It enables us with unprecedented connectivity and functionality in all aspects of our lives. We work, play, learn, and overall live differently with the tools technology provides. At the same time, we are also vulnerable in many new ways and the “bad guys” can leverage both this new technology as well as the ways we use it. Being more connected means it’s easier to connect to you. Having more functionality means there are more tools available to get to you.

Technology has become so integrated into our lives that it is no longer practical to be safe from technology attacks by simply avoid technology altogether. To be safe, we have to be smart about how we use our technology and we also have to be aware of how bad guys can use these tools against us.