

Essential Strategies for Technopreneurs

Dr. Hamed A. M. Rushwan, B.Sc-BATS, Ph.D.

Chapter Six

How to survive surveillance!

Surveillance costs industry and Technopreneurs billions and billions for intellectual property loss and projects theft. The ridiculous low investment for surveillance makes it a growing business for many who used to make their life on misery of others. Especially if they can get a million dollars in sales for every few hundred dollars spent. To them it is much better than drugs, illegal trafficking and gangs, also decorating this unholy activity with a patriotic theme attempting to make it holy and encouraging their family members to spy on their own friends. The difference between authorized legitimate monitoring for public safety and unethical surveillance starting from stealing secrets and watching victims in very private situations is like a very fine hair, always missing or shaved on purpose.

Surveillance is the profession of ZERO ethics code, and can recruit the last person you can expect.

You owe it to yourself to protect you self, never under estimate how important your work is or to think you're still in the beginning and have nothing important developed yet. Surveillance can be set on you for years and for few dollars a month, you consider yourself a Technopreneurs you got to adopt an anti-surveillance strategy and make it part of your life!

Do not take it racial and do not get paranoid, but for more than three years a Muslim family with young autistic child been under Audio/Video surveillance using bad neighbors with the authorities knowledge. The bad neighbors failed to find anything wrong with the family so they started using the surveillance equipment to know when the family went to sleep and come to bang on their doors after midnight, running in the family's residence with there trucks and use the surveillance to ruin their business, Spy is a person with criminal mentality and

Zero ethics. It may harm you despite you are clean. Just to proof that he wasn't wrong in the first place it continues, instead of compensating you and Apologize. So do not be the next victim or even live bait.

Surveillance in the new millennium is not a car following you or a bunch of felons setting in your basement with big eavesdrop speaker connected to your phone line with gigantic audio recorder big enough to get your whole desktop computer inside it. No, it only need tiny GPS tracker for only few hundreds dollars to track your car and a \$15 FM Phone connector transmitter to replace your existing one in your office in less than 10 seconds while you were answering the door. Never leave that strange visitor beside your desk. Well, even exchanging the phone card is an easy task for any phone company ex-employee from your phone box outside your home or office. Beside of-course accessing your non-password protected telephone company voicemail, also it is not carrying the important conversations beside the ocean loud waves, new electronic filter synchronizers with lips reading computer can bring more clear than you talking. In fact you will find in the next section that your white wall glass skinned lab is safer than other places. Defeating surveillance won't be achieved by using anti bugging device only. It will be achieved by adopting a certain behavior and strategy.

The Essential part of this strategy is to judge and characterize the size and the danger of the threat. Exactly the same way you judge and characterize a prospective client, How far can they go and how

far can you go to protect your hard work? And here is another golden rule, "if surveillance only cost few thousand dollars to steel millions, defeating that few thousand dollars surveillance would cost only few Hundred dollars and little efforts", Also the reward is great: safety, peace of mind and also you may win a little piece of gadget can lead you to who is trying to sabotage your life and bring them to justice and then ultimately to the civil court to pay up.

There are major surveillance tectonics need to be manipulated and defeated by your strategy:

Hacking your computer/server/data storage space, through direct control, virus, adware, Trojan....etc.

If you can always keep one computer off the Internet and other networks, as your vault, and only transfer from it and never to it, and always through disks/CDs formatted on the same computer. I know it sounds basic and little obsolete, but it's never defeated except by accessing the actual computer manually, we'll cover this later

The other computers got to have Firewall as Zone Alarm, anti-virus as Norton, adware removal installed all the time, as for the adware removal software you will find many of them are produced by spy firms, It make sense. They are the most experienced in spy tools, producing it, then producing a tool to remove every other spying bug but theirs. Most of the time installing their bug on your computer and update it with transferring you data, to defy this, you'll need to install more the one spy remover program, so every one will remove the bug of the other program!, also when they contact

the Internet, if you chose to allow them to do so through your firewall, watch that they are receiving not sending all the time!

Consider dedicating a less demanded computer station only for emailing activity and away from any of your Internet activities, this will pay back in better security.

Update your computer operating system regularly and on demand. Many threats get fixed in the original system like windows for example just days before the global spread of the threat. Many who update the system regularly against latest security threats really get away safe every time.

Never leave your computer online all the time, at least turn engage Internet lock through your firewall. Many spy detectors can detect registry manipulation, turn this option ON.

When updating your site, scan your local web folder on your computer for spy wares. Erase the whole web folders on the webserver and re-upload the whole site on a clean server. Watch your computers performance. If it slows down after visiting a website, you probably caught spyware, clean the cache using professional software. If it does not improve the speed, run a system scan then reboot.

Never allow search tool bars on your browser, they track your surfing. Also nosy programs that claim automatic update, except your own trusted platform/Operating System OS, firewall, virus protection, every other program got to ask for a permission before contacting, being on the net is like being on a downtown street so any thing could happen, so be ready.

Keep a separate drive or a partition from your existed drive for your data, and a copy of your original C or booting drive updated. Every month, delete and format the whole C drive and copy the original from the other disk/partition/CD to it, you will get amazed how your computer will do better and How felons loose your trace! If you are that type of closed in a hurry by the end of business day, set your computer to clean traces, check viruses, sweep spyware overnight as scheduled maintenance. If you prefer to manually shut-off the computer and lock it, set this maintenance during launch time. Do not carry multiple days in business with spyware transferring your data. It is like working for your enemies.

Use encrypted email software between you and your partners, Do not repeat what happened over the phone on the email for the same client. Do not send back the same email back and forth as reply to all the time. Simply one of these emails can reveal the business preparation for a month.

It is a good practice to make the data hard drive removable or even all the hard drives and lock them overnight. While you are away your 3 months hard work cad design can be taken in 3 minutes data transfer over your printer port, remove the drive.

Bugging your phone/fax/cell

Now this idea depends on the level of the threat. This will determine the amount of sophistication as follows:

Scanning your place with a cheap transmission detector will do the trick to get rid of small telephone receptacle connectors or FM

transmitters installed by trade amateurs. The transmission detector is all over the net and getting cheaper everyday. It detects every high radio transmission as cell phones in un-authorized areas, as well as wired people and bug transmitters. It is simply a regular pager without a tuner which buzzes in the existence of every radio transmission with higher deference of potential than 20 mv. Even this unit can be adjusted through sensitivity adjuster knob. A directive antenna can be added to show you the direction of the transmission. Remember, this detector can't detect issues of online phone bugging, sonar transmitters, programmed transmitter that transmit on demand, except if you leave it ON with adapter at all times. Maser and VUHF "very ultra high frequency" are not all that the detectors are not designed for. The same is for Ultra low frequency, analog and digital scanners which is good for your wireless and cell communications. Mind that the simple baby monitor can be intercepted easily by a good antenna and good RF booster. At least leaking some information about you and people around you. Also if you are using wireless cameras to monitor in/out your property the same concern applies, so wired cameras can do a securer job.

Never transfer information over analog systems, even in a home wireless system. It's just a disaster, especially if you suspect Bugging. Transfer partly false data and watch the results.

Never lend your cell to anyone. It may come back bugged, not by the used but by someone using him or her.

If your project is big, then setting a frequency analyzer antenna

connected to the laptop is a valid option. This setting will analyze all the frequencies around your property and catch unauthorized transmission for immediate investigation. The same is done by using oscilloscope analyzer for every landline coming out of your property - even the power line. As carrying the Surveillance data over the power line to your Neighbor is a common practice, this will get the IN and OUT under control.

Defeating audio/video infrared in-house surveillance

As a rule of thumb, infrared cams detect infrared cams, nightvision goggles/glass, infrared cams. The famous Sony night camcorder, and even the IR filter black glasses can see part of the IR spectrum that regular human eyes can't see. They simply convert the IR into near green photo and in color in updated types, simply you will see the laminating IR LEDs that luminous to the camera lens to spy. For regular spy cams, you can detect the internal frequency by a bug detector, but if it is shielded you can detect the transmitting frequency from 900 MHz to 2.4 GHz, but if it's wire and not wireless, using a metal detector will get it. If it uses fiber optics instead of the metal wires it will not go far until it reaches the electronic board with its recognized frequency to the bug detector.

Do not put your office in the front of the parking lot. It is so easy to eavesdrop through the glass window with small laser vibration detector and an ultra sensitive direction microphone. I saw it myself, the bidding price and even some ingredients was revealed in one

meeting. The Technopreneur suspected his visitors but they were innocents.

Please watch your discussion and always remember which information went to who. And who is entitled to which level of information. Please do me a favor, never volunteer with your own personal or research information.

Never meet people in your working office, just make a general corner or fixtures in a clean room for meetings, exchange files, discuss business. Never let visitors in your working office. Neither your courier delivery or Pizza boy, because your working office is not an open exhibition for your work.

Your lab wall should be all white with nothing hanging or a wall clock. A spying wall clock is everywhere and looks exactly like yours, use your hand watch for timing and spray your lab's wall with simple white paint once every few months. This will block pen hole hidden cameras, use you own instruments and do not leave one instrument outside all the time. This can be used for hosting the surveillance camera..

If you skin the Lab wall with IR blocking glass, like that one for winter nursery, or fill it with refractory materials or black color cloth or used tire rubber, these will block the outside Energized Infrared imaging.

Car GPS tracking

For Bulk Materials pick-up, use rental trucks. This will keep your car new and the tracking just in the rental agent parking lot you can

also change the agent next time, seeing your easily recognized car specially with the company logo in the front of the supplier's front door is just invitation for peaky Dave to step in and say hi... I just saw you car outside. If you must, leave your car away at least fifteen yards " GPS accuracy" and walk. Use your other registered company to buy and receive the invoice then settle this between your two companies for the tax proposes. If the surveillance reached your tax files, you'll need to change province/state or even cars..

In the rest of this chapter, you will read about:

[Eavesdropping your associates, alliance and suppliers](#)

[Your Mail and Courier](#)

[Games, Games and more new Games! Welcome to the club.](#)

[Sort your Garbage](#)

["Choose the Right Environment"](#)

Plus very informative other chapters of the book:

1. Zero Budget prototype
2. Your Corporation, Your identity
3. The Internet, Your Empire
4. Barter, turning the table on the emperor's gold
5. How to turn Challenge into Opportunity and down-time into R&D
6. How to survive surveillance
7. The art of Success

Order Dr. Rushwan's newest book for Electronic Delivery at

<http://www.RushStar.com>