

Enemy of the State of Privacy

Robert Ing, DSc, DLit, FAPSc

Full Article Available at www.drroberting.com
Copyright © 2004, 2005 Dr. Robert Ing, Toronto, Canada

In the 1998 movie, "Enemy of the State", actor Will Smith's personal privacy is invaded by his own government using high technology devices planted in his home, office and even on his person. Sounds far fetched? The technology does exist to do everything portrayed in the movie and much more. The only difference between the movie and real life is that unlike the movie where government agents physically entered the home and office of Smith, this is not necessary to breach the privacy of any citizen.

If you are like most individuals, you have unknowingly permitted yourself to be tracked, documented and your privacy breached in exchange for living a life of convenience. When you sign applications and agreements for your credit cards, bank accounts, vehicle leases and mortgages have you really read the fine print? The fine print in most cases states that you give your permission to have your personal information collected by, "exchanged" with, and even sold to third parties throughout the course of your business dealings. Do you belong to a reward points or discount program? The fine print of the agreement may allow program operators to track your spending habits (where and what you buy), allow them to share and even sell this information to third parties and put you on mailing and telephone solicitation lists of companies you've never heard of.

While this may seem more of an inconvenience than an invasion of privacy consider the case of Mr. X. Mr. X had signed up for a reward points program linked to his credit card. This meant everywhere and every time he used his credit card he would get points for all of his transactions to be used towards vacations, gasoline and a new car. Mr. X was in line for a promotion with his firm, a major multi-national corporation. As part of the selection process he would have to submit to a background check and security clearance. The firm conducting the check performed what is known as a character lifestyle check and through their sources were able to obtain a record of Mr. X's spending habits over a two year period as documented by the reward points program he had enrolled in. It was noted by an entry on his spending record that he had on one occasion frequented a small retail establishment whose operator had been convicted of child pornography. As a result, Mr. X was not given a clearance for the promotion and was later released from the firm's employ. Further investigation found that the establishment in question was a convenience store chain where Mr. X purchased a box of chocolates for his wife's birthday. This was the one and only documented time he had entered this establishment.

Similar tracking of individuals is also done via their personal computers. In this case, most individuals are all too quick to breeze through the Terms of Service posted on websites and in software and as a result surrender their privacy all too easily. People who do any form of online commerce from ordering merchandise off of a website, to online banking and stock trading are often tracked by having small files placed on their computers without their knowledge, known as cookies to gather and track personal and personal preference information. By accepting the Terms of Service users agree to have the cookies placed on their computer. Although the word "cookie" may not be specifically used in the text of the document. Cookies, also known in the computer security world as Spyware may provide information about the computer owners name, address, telephone number and e-mail address all culled from information provided by the users themselves when they first registered their computer operating system and software. Additional information may be obtained on the type of software and computer used, websites visited, Internet searches performed and total time spent at the computer.

As well, Internet Service Providers and e-mail providers may also keep tabs on users by monitoring account activity. Account activity of this nature would include received and sent e-mail addresses, websites visited and an inventory of all of the software installed on the computer. Information obtained from the use of Spyware and the monitoring of account activity are routinely justified in the corporate world as processes designed to selectively send specific advertising offers that users may be interested in based on their "tracked" previous purchases or activity and to ensure the quality of services delivered to users by monitoring user access activity.

However, information accessed by or sold to the wrong hands could be devastating to an individual. An example of this occurred when Ms. Y, a grade school teacher had her name come up on an e-mail mailing list associated with a contraband prescription drugs operation that had been seized during a raid. Although it had been later found that Ms. Y, like many others on the list were simply targeted victims of a mass e-mail solicitation list, the fact that information from her e-mail account provider indicated the receipt of a message from the operation and a sent reply message that could have raised further suspicion. However, given that the e-mail activity log did not store the body of the message and Ms. Y's explanation of the reply simply being a request to be removed from the mailing list seemed credible given no other communiqués were logged. More importantly, Ms. Y would have never been placed on the list if the health related website she registered with as a user had not sold her information to an e-mail marketing firm who later re-sold it to the contraband drugs operator.

While most may find comfort in privacy laws directed towards protecting personal information collected by firms in the course of doing business with and servicing their customers, there is little refuge or comfort when an individual is confronted with accepting the terms of the fine print in their user agreements or to be forever without service.

So you say you can't imagine your life without your cellular telephone. If you are like most people, you keep your cellular on as you go about your business every day. Did you know that using just the signal from your cellular telephone and its unique electronic identification number that your whereabouts within a 4 city block radius can be easily time stamped to the second, dated and determined. This capability of passively tracking and recording the whereabouts of individuals has been effectively used as supporting evidence to place or not to place suspects at or near the scenes of crimes. Call records of cellular telephones have also been instrumental in keeping people in and out of jail as well when it comes to alibis. The same holds true for the detailed billing feature of monthly cellular bills, you know . . . that listing of date, time and telephone number called or received. The detailed billing feature has been the demise of many an unfaithful spouse. As one U.S. intelligence official once said, "... cellular telephones are one of the greatest surveillance advancements of our time. They enable unobtrusive surveillance of practically anyone at anytime."

So perhaps you're thinking you should just turn your cellular telephone off and maybe spend some time just taking a walk to the mall and having a quiet cup of coffee in the food court. Look up, way up! Do you see those shiny black domes in the ceiling, or those boxes with black glass or the obvious camera in a white or grey box hanging off of a post? You see them on street corners, in malls, office buildings, transit stations and highways. You are under surveillance and your presence is being recorded, dated and time stamped. Security video camera surveillance is more widespread in major cities than the public thinks. If you live or work in downtown Montreal, Ottawa, Toronto or Vancouver a typical one way trip will cause your image to be recorded an average of 9 times by 7 independent video surveillance systems. 85% of video surveillance systems are owned and operated by corporations for use on their property such as malls and office buildings, with no legislated guidelines on what they can do with this recorded surveillance data. Security video recordings are kept an average of 3 months before they are erased or purged.

To get away from it all you may consider a quiet drive in the country, far removed from the hustle, the bustle and those privacy invaders but . . . you can run but you can't hide. Most new vehicles come equipped with a safety option that allows you to be in instant live two-way communication with a dispatch centre should you have an accident or just get lost. This service will not only talk you through your emergency but also unlock your doors if you are locked out and will even pinpoint the exact location of your vehicle using GPS satellite tracking if it is stolen. GPS satellite tracking is the same technology used by the military and just like military targets; your vehicle's location can be determined within 3 metres. Similar in-vehicle security only systems also use GPS to track and locate stolen vehicles. This technology is not only available as an option when you purchase your new or used vehicle but is now standard equipment on most vehicles you may rent for that weekend getaway.

Although the safety and security benefits of these devices are numerous, so are the privacy risks. One area of concern is that the in-vehicle two-way communication feature can be activated by the dispatch centre without the vehicle occupants being aware that every word they say can be monitored and recorded. Moving vehicles and their parked locations can also be determined without any occupant knowledge. During the past few years there have been documented cases where law enforcement agencies have utilized such means as an aid to conventional surveillance methods.

The real ability to put an average citizen under surveillance, collect personal information and invade privacy used to be the sole domain of governments about 25 years ago. However, with the accessibility to, and affordability of technology, the ability albeit in a limited way to track and create dossiers on individuals by corporate snoops and even private individuals is an easy task. Bearing in mind that unlike governments, private corporations and individuals acting alone or on behalf of someone else are not bound by such stringent controls to protect the democratic rights and freedoms of citizens. While privacy and personal information laws do dictate how businesses must store and disseminate information pertaining to their customers, loopholes are easily created by fine print user agreements and the acceptance by the potential customer of the user agreement is demanded in order to obtain service from the business in question.

Unlike governments, private corporations and individuals are able to operate in grey or open areas of the law in collecting and comparing information from other private corporations and individuals with minimal checks and balances. Furthermore, when one considers that despite legislation and codes of conduct, the bottom line is that there will always be someone who knows someone, who knows someone else who can obtain the required information through a low level contact with access to the requested information. If this sounds funny, don't laugh because any street savvy privateer will reluctantly admit that this is how things really get done.

Personal privacy must start and stop with the individual. You must carefully review service agreements before accepting them. Is the service, product or convenience you are interested in really worth giving up some of your privacy? Do you really want to give someone the potential ability to track your movements on a daily basis?

Just a final thought . . . don't be surprised if a total stranger comes up to you one day and can tell you what colour you prefer in underwear, where you shop, that you take the long way home and that you would be able to call your mother more often if you didn't stay so long on your computer. Only you have the power to not let this happen.

About the Author

Dr. Robert Ing is a forensic intelligence and technology crime specialist. He may be reached at 416-563-6958, or via e-mail at Ring549@aol.com, www.drroberting.com