ASPECTS OF SURVEILLANCE

Dr. H.B. Wolfe
Information Science Department
Otago University

Introduction:

If you thought that you were safe from being watched by anyone, well, think again. Modern surveillance tools and techniques are virtually impossible to detect, therefore, if it is happening to you, you will not know it until the watcher decides to let you know (or never, as the case may be). It can be easy to dismiss events going bad as the luck of the draw; however, knowledge of your plans allows others to be in a position to act beneficially on their behalf, thereby disadvantaging you and most probably even without your knowledge.

Paranoia you say. Well maybe, then again, maybe not.

Many people believe that giving up privacy for a little perceived safety is worth the loss, however, in practice the loss can almost never be recovered. There is always an asserted benefit to be obtained, a plausible cover story. Remember that surveillance in the hands of the "authorities" becomes a means of social and political control. Knowing that you are being observed inhibits your actions. Consider your behavior when you know that you are driving by a traffic camera. Surveillance in the hands of an enemy or competitor may mean that your plans may fail – you may fail. Consider your behavior in places where surveillance cameras are being used – and you are aware that they are there.

Some would argue that the cameras inhibit crime because the criminals too change their behavior around that kind of surveillance. However, I believe that you will find that crime just moves to another place – it doesn't stop. A good analogy is rearranging the chairs on the Titanic. The outcome will inevitably be the same.

There are plenty of laws and international declarations and covenants that guarantee your privacy. New Zealand has such laws and is a party to these declarations (for example: the Universal Declaration of Human Rights – which in Article 12 guarantees every person's privacy). Many of these either govern the authorities' behavior or inhibit it somewhat, however, surveillance can and does take place with or without appropriate official authorizations (in some cases a warrant). The comments in this introduction do not even begin to cover the kinds of intrusions and abuses that can take place by the unauthorized use of computer and other electronic data. That is a whole new kettle of fish.

Surveillance: What Can They Do?

Your movements within your domicile can be watched using heat sensitive equipment. A watcher can know of your every movement. The sounds that occur within your domicile can be captured by a number of different means and transmitted, also by a number of different means, to the watchers wherever they are. This information can be

recorded for later analysis or potential use in future investigations. Video cameras are small enough and cheap enough to be secreted almost anywhere and the images captured by them transmitted by various means to the watchers, once again for analysis or use in future investigations. The notion that these techniques are expensive or technically sophisticated to the point of needing specialist operators (watchers) is spurious. The kinds of technology needed to perform this kind of surveillance are simple to place and to use. You just have to know where to obtain them or how to put together such devices. There are even kit sets for building bugs that are perfectly adequate for some surveillance tasks. The costs for these are less than NZ$50 per unit.

It is almost impossible to find a spot in Washington where surveillance cameras are not present and they are proliferating. The same is true of London and other cities as well. In New York City, a survey of eight blocks was done and more than 1,200 cameras were visible. No one knows how many were not visible. There is a whole family of surveillance cameras that can easily be hidden and invisible to the human eye. They can also see in the dark if the area is illuminated by infrared light (which is also invisible to the eye). So even in the apparent dark you can be watched with impunity. We are told that this is progress and we are safer because of it.

The laws that govern surveillance activity are vague and not enforced well with little oversight. But more important than that is the fact that placing and using a bug or camera is REALLY hard to detect – no matter whether it is placed illegally or with the appropriate authority (warrant). Protecting yourself from this kind of intrusion/abuse is difficult at best and impossible at worst case. With certain kinds of devices, entry to the target premises is not even necessary.

Those in authority will say that they are governed by rules and that they cannot use surveillance techniques without the appropriate authorizations (in some cases a warrant). Others in positions of power are not encumbered by any requirements for warrants and even if they were discovered, would be exempt from prosecution. We all know that those in power historically have abused their power and yet we are asked to trust that now for some curious reason the long lessons of history do not apply and that the power that they wield will not be abused. Most people would like to believe this and perhaps it is just as well that they do. Those in power most certainly would like you to believe this.

Roman satirist Decimus Iunius Iuvenalis (also known as Juvenal 65-127**AD**) once said: "Sed quis custodiet ipsos custtodes?" – who watches the watchers? The question was on the mark then and is also on the mark now. Why should we trust them? Think for a moment and honestly consider is there a single politician that you would trust?

It may be worth mentioning that in *Discipline and Punish: The Birth of a Prison*, Michel Foucault wrote "Hence the major effect of the Panopticon[1]: to induce in the inmates a state of conscious and permanent visibility that assures automatic functioning of power." The notion of "automatic functioning of power" really also applies to public surveillance. Some would argue that you cannot expect privacy while in a public place, however, one can turn away or speak softly in order to obtain some privacy in a public place. Surveillance equipment can easily circumvent that autonomy. While you could choose to exert your autonomy and turn away and speak softly,

[1] *The Panopticon* – a perfect prison where prisoners would be under constant surveillance

surveillance equipment can be very sensitive and hear those private conversations anyway.

So the main question that we should all be asking is how, when surveillance equipment and techniques are capable of observing and recording all, shall we obtain real privacy? Unfortunately, I'm not so sure that there is a positive answer to this question. Perhaps we might force the politicians (I'm not sure how since each has their own private agenda once elected) to make surveillance unattractive or unacceptable: morally, ethically and/or legally. Perhaps the watchers might be punished for watching.

Computer and Other Electronic Surveillance

Physical surveillance can produce information about what can be seen or heard, however, much more pervasive and, in fact, intrusive surveillance can now be carried out through the use of computing technology. For a moment, let's think about the myriad of different databases that proliferate within modern society. There are those mandated by various government entities and there are those created for administrative and marketing purposes. Within government circles we are constantly told of the advantages of being able to combine the databases that they hold. Their plausible cover is that it will enable the reduction of benefit fraud, tax evasion or some other apparently attractive cause.

At this point I am compelled to reiterate Foucault's statement that "continuous and permanent visibility assures the automatic functioning of power". In other words database linkages with continuous and automated surveillance assures the means of social and political control.

We are already inhibited from using words, in the name of political correctness, that supposedly various special interest groups find offensive. My response to that form of censorship or behavior modification is: get a life! Everyone has the right to think whatever they wish. It is deeds that count and as long as we do not harm others then we should be left alone to interpret available information and make judgments and form opinions of our own. Certainly without the interference of government who, we are told, are there to serve us.

Data Surveillance: What Can They Do?

Think for a moment about what information you routinely supply to complete strangers. Cash a check and you must provide your name, address and phone number along with some form of "acceptable" identification. The cover is to protect the organization accepting the check and if that were all that it was used for there might be no objection. However, what happens to the information supplied? Is it ever used for any but the purpose stated? For every credit card transaction, much detailed information is transcribed and stored for later use (such as time, date of purchase, items purchases, location of purchase, amount of purchase and much more). If it were only used for billing purposes there might be no objection. However, this information is analyzed and used for individual and demographic marketing purposes. This enables the user to take advantage of your predilection for purchasing types of goods. Their cover, of course, is that they will provide better and more tailored marketing to you (somehow that is supposed to be to your advantage).

Let's just list a few places and types of data routinely stored about you. In no particular order we have telephone information (who you called by number, when and how long you talked). If you have a cell phone it is possible to maintain physical location information for every cell phone active (in other words your exact movements minute by minute – within a few meters). In the US all cell phone geographic locations must be immediately available for 911 (emergency) calls. If the data is available for emergencies it will also be available for other unspecified purposes providing opportunities for abuse. Your exact geographic location minute by minute may be of interest to any number of organizations – both governmental and private. How would you feel about receiving a cell call informing you that you were in the neighborhood of a store that was to have a special sale right now?

Medical information is stored to help protect your health, however, there is a strong movement to have everyone's DNA tested and recorded in a database. If such a database (DNA) were to exist, who would have access to it? Once certain genomes were mapped, identified and their attributes described, it would be valuable for insurance companies to know that certain individuals were prone to certain diseases (and we all know that premiums for those people would rise as a result). Employers who might have access to such information may decline to employ people in various categories for reasons that have nothing to do with qualifications or work performance history. Then there are educational databases where your performance throughout your formative period can be recorded for later processing and assessment. When we get to financial databases, we get into another sensitive area. In America ("the land of the free, home of the brave") bank clerks are admonished and required to report ALL "unusual" financial activity of ALL of their customers (to the Department of Treasury). Maybe "free" is the wrong word. Free not only means the ability to do what is within the law without interference but also the ability to be left alone.

Without direct evidence of a crime or without demonstrating probable cause, why should anyone's financial transactions be anyone's business other than their own. Why do various countries require that you report when you have more than a given amount of money in your possession while traveling? Why is that any of their business? No one asks this question because we're afraid to draw attention to ourselves, and that by doing so we will be subject to consequences of one kind or another. Is the demand for this private information not interference with our freedom to be left alone? Is there any law broken by having more than a set amount of cash in your possession?

There are many more databases: the list goes on and on. What happens when all of these are combined into a single repository of information about everyone? Will this not inhibit our freedom to act? Will this not provide the means of social and political control to be instrumental in changing people's behavior: social behavior, economic behavior, political behavior? Individuals will inevitably just not do anything that might be deemed to be "inappropriate" and reported by the watchers (those who control the databases) to their masters. Probably, the most important question of all is: who decides what is "appropriate" behavior – socially, economically, politically?

In George Orwell's *1984*, he described a world where there was no privacy. A world where every action of every citizen was observed by Big Brother. Where people were inhibited from using words that were unacceptable to the thought police. It would seem that the title of George's book was just a little premature. Governments, politicians and law enforcement are relentless in their pursuit of control. We are

inexorably on the road to building such a surveillance society today. Whether it is too late to change this trend remains to be seen.