National College of Art & Design

Faculty of Fine Art / Painting Department

"Our Society is not one of Spectacle, but of Surveillance"

by

Daniel Cullen

Submitted to the Faculty of History of Art and Design and Complementary Studies in Candidacy for the Degree of B.A. Fine Art / Painting

1995

Table of Contents

Introduction

"*The 20th Century is the filmed century...the whole world is on film, all the time, spy satellites, microscopic scanners, pictures of the uterus, embryos, sex, war, assassinations, everything.*" (Don DeLillo...'Running Dog'.)

In this thesis, I will propose that we live in an 'invigilated society', one in which we are as individuals subjected to growing and unremitting surveillance by state and corporative agencies.

I will describe the contemporary technologies of surveillance and information gathering and their implications for individual liberties.

In Chapter One I will attempt to describe some aspects of the evolution of the technology of surveillance, information gathering and storage, from the 18th Century through to the present day use of computers, video cameras, telecommunications etc...

In this chapter I will also consider Foucoults use of the term "physio-political" to describe the instrumental use of optical technologies. Foucoult sees the 'Panopticon' of Jeremy Bentham (1791), whereby the machinery of power becomes automated and bars are replaced by visibility - as the progenitor - of todays surveillance technologies.

The principles of the 'Panopticon' have their contemporary application in the use of video surveillance in public places, the developement of 'intelligent' cameras, and the computerized storage of information on literally everyone.

The new technology by necessity has created its own intercommunicitive language and a whole new vocabulary to describe its processes. This new intercommunitive language must of necessity affect the users perception of reality in as yet unforseen ways. The new 'media-ecologists' have coined terms like 'information overload' to describe a phenomenon which presents real problems as vast amounts of computer storage space become available - with a commensurate human compulsion to fill it - a condition which is also described as 'infomania' .I will be looking at the implications of 'Textual Cleansing Software' ie; how computers and their users can inadvertently decontextualize information which passes through the computing process leading to possible distortions of meaning.

In Chapter Two I will address ' The hour and the moment of the Lists '. ' Infomania' , the compulsion to index, categorise and catalogue, which when applied to peoples private lives raises issues relating to ethics and legal boundaries. The Criminal Justice Bill, recently introduced in the United Kingdom, greatly facilitates this process of personal information gathering.

The activities of Sen. Joseph McCarthy's " Commitee on unAmerican Activities " which carried out the 'Anti-Communist'

witch hunts of the 1950's in the United States proves that Liberal Democracies are not immune to ideological inquisitions.

In the light of this, the existence of vast amounts of comprehensive information on all aspects of people lives makes the questions of ' Who compiles it ?', ' For what purpose do they want it ?' and ' Who has access to it ?', ones of critical importance.

In Chapter Three, I will examine the activities of two major intelligence gathering agencies - specifically the ' National Security Agency ' of the United States, and the ' Government Communications Headquarters' of the United Kingdom, and their SIGINT (Signals Intelligence) activities. I will examine how their activities impact on smaller geo-political entities, taking Ireland as an example.

Finally I will examine how surveillance has become an intrinsic aspect of modern technological society, and why it often enjoys the passive and even the active support of the mass of population.

This latter fact makes it more difficult to see how counterbalances to uncontrolled surveillance can effectively be put in place.

In my proposition to show how we live in a heavily invigilated society, I recognise that some of what I will put forward occupies the realm of theory in so far as it can not (due to its very nature) be easily proven. However in an atempt to avoid raising any 'Orwelian hares', I have made a determined effort, only to make

reference to technologies, and their applications, which are already in use.

Chapter One

"Our society is not one of Spectacle, but of Surveillance," wrote Michel Foucault in 'Discipline and Punish: The Birth of the Prison.' Spy satellites read licence plates from astronomical heights. Motion-sensing cameras swivel to follow the movements of bank customers, convenience store customers, people in lifts. Behind two-way mirrors, security personnel lie in wait for shoplifters. Thumbnail-sized video cameras may soon record all transactions at automated teller machines. It is now possible to go into a "spy shop" and purchase night vision goggles, briefcases with secret cameras and pairs of glasses with rear-view mirrors.

"On the horizon of the next millenium" writes Mike David in 'City of Quartz', *"an ex-chief of police crusades for an anti-crime "giant eye" – a geo-synchronous law enforcement satellite"*. For now, though law enforcement agencies will have to make do with marginally less Orwellian devices, such as the surveillance technology of the Los Angles Police Department airforce ie; French made aerospace helicopters whose forward looking infra-red cameras are extraordinary night eyes that can easily form heat images from a single burning cigarette, while their thirty-million candlepower spotlights, appropriately called "Night Sun" can literally turn the night into day.

In Discipline and Punish, Foucault used the term 'physio-political' to describe the instrumental use of optical technologies by

disciplinary societies, he predicted their introductiuon would inevitably lead to a state of unremitting surveillance. Foucault termed this phenomenon "Panopticism" after the institution set forth by Jeremy Bentham in Panopticon (1791). Bentham was an 18th century philosopher of the Utilitarian school, who conceived of a revolutionary prison consisting of a cylindrical framework ("an iron cage") whose cells, rising tier upon tier, gave on a central courtyard dominated by an observation tower. Sunlight, streaming through the open ended cells and pouring down from a skylight in the annular building, would turn each prisoner into a dramatically back-lit figure whose merest movement could easily be seen. He devised special reflective lamps in order to ensure that the cells would be flood lit 24 hours a day. The warders in their observation tower would disappear behind an elaborate system of blinds, partitions and zig-zag openings designed to prevent light or shadow from betraying their presence.

The Panopticon, whose name is derived from the Greek word meaning "all-seeing", accomplished its objectives with the simplest of means: optics, geometry and architecture. It facilitated the management of the many by the centralised few or one, or none, since the prisoners had no way of knowing when the overseers were at their posts and therefore had to assume that they were under observation at all times. Basically it was a system which sought control of the mind as well as control of the body, the idea being that if the prisoners thought that they were being watched continually, they would abandon any ideas of transgression. Bentham spoke of compiling lists of transgressions which would be presented to the prisoner later. He described his prison as a

device for "grinding rogues honest". Thus, the machinery of power becomes automated, bars are replaced by visibility.

Bentham envisaged cities built upon Panopticon lines and, in fact, his Panopticon is prototypical of the modern office, factory, school, asylum and, of course, penitentiary and any other *"conspiracy of the architectural and optical"* (Mark Dery...'Terrorvision') which creates a space in which behaviour modification is effected through unremitting surveillance. In fact, the very city streets, it would appear, are adapting to this "Panopticism". In the words of Dr. David Wilson, Governor of Woodhill Prison in England, *"as I go out into the streets increasingly I see the images from the work that I do in a prison, as though the community were becoming a prison"*. (D.Wilson...'Metropolis')

He was referring specifically to the relatively recent spread of video surveillance in public areas in cities like Newcastle, Birmingham and London but also to the implementation of video surveillance by local councils in smaller communities throughout Britian. In Ireland – first in Cork and now in Dublin and soon in Limerick, police video surveillance cameras are becoming more common perched on very high poles or on the top corners of buildings around the city centre like some strange breed of bird. It is not unreasonable to say that the camera is becoming part of the fabric of the city, but what price do we pay for this security? In a sense, as David Wilson said, the community is becoming a prison. "When technology reaches a certain level, people begin to feel like criminals... The facts about you and your whole existence have been collected... It's the presence alone, the very fact... of

technology that makes us feel we're committing crimes." (Delillo: Running Dog). With Panopticism, since some of the transgressions will be acted upon, the prisoners have the ever present awarness that invigilation is taking place. The psychological climate of being invigilated constantly (or of believing that one is being invigilated constantly) becomes internalised by the subject, who is now to a great extent invigilating himself. Today this process can be seen to have its 'economic' extention, in the fact that amongst the ubiquitous video cameras there will be cheap fakes. The revolving 'sensor' on the T.V. detector van *may* be a fake, but it is sufficient to bring in a harvest of licence payments at low cost.

In the black & white low resolution pictures of most security systems the shadowy time lapsed human images are all those of potential 'perpetrators', and we all appear on these screens countless times. In fact, the average person has probably put in more screen hours than most movie stars.

Video cameras, remotely controlled, have a heavy air of impersonality. "Authority has a cold and distant face" (Wilson). this can serve to alienate a public from the institutions involved, and can also lead to an air of fear and mistrust. It removes the responsibility to take care of each other. Now an all-seeing eye does the job for us. This surely leads to a downward spiral which, of course, the authorities try to correct by implementing even more pervasive security measures. Measures which are even more 'cold and distant' than before, because no longer can we be sure what is watching you. Security cameras are becoming standard both in public and in private places. Soon they may

even be required. Why? Ostensibly because they want to recover losses in cases of theft, keep insurance premiums down, monitor petulant employees and keep intruders out, etc. But the new genre of video cameras now coming out of the labs do a lot more that. They could be said to be intelligent. They can recognise faces, motion, and other interesting characteristics. In fact, they behave a lot like the human eye, with intelligent preprocessor abilities.

Intelligent cameras are needed because a security guard or policeman cannot monitor dozens or hundreds of video cameras in a large building or city. Intelligent cameras use artificial intelligence-based object and motion recognition. They scan for what a trained security guard looks for: certain motions, clothing, faces, the presence of people in off-limits places. Instead of watching 100 cameras, only a few at a time send pictures. A single guard or computer can deal with that. In fact, a steady data stream from multiple intelligent cameras can be uploaded to computerised monitoring facilities anywhere, coupled with other automated observation systems. The next big development in intelligent cameras will be 'content addressable' imagery. That means that they will automatically detect the content of sophisticated patterns, like a specific person's face, by matching it against a digital list. New software that can even run on cheap personal computers makes this possible. MatchMaker from Herated Systems, for example, automatically recognises and categorises in realtime 'targets' - untouched by human hands and tied into a centralised monitoring facility. This technology is inexpensive, easily reproducable and will be part of standard

equipment for fully automated on-site visual and infrared surveillance. These smart cameras are also getting incredably tiny as well as low cost. For example, the Imputer from VLSI Vision Ltd. is a credit card-sized device that fits in the palm of your hand. It incorporates realtime image enhancement, feature detection, and even an optical library of pre-stored feature data so that the camera can independently recognise a specific face. It can also download its captured visual data via a telephone line.

With very few chips, intelligent cameras can now be mass-manufactured like pocket radios. No need for security personnel – they can be linked to a computer surveillance monitoring and data base system.

When the technology becomes so cheap, tiny and powerful, and no guards are needed, they could be secretly placed on every street corner, phone box, waiting room, office, wherever.
This is Panopticism in a cybernetic (systems control) society.

Cybernetics only really took-off with the advent of Fordism. Ford himself had a compulsive need to control, he had to know everything about his system of production. There was no room for variables. This is a 20th century phenomenon which has carried over into almost every aspect of life in the post-industrial world. Now, instead of systems of production, we are dealing with systems of information where any and all variables, or 'unknowns' must be eliminated.

The enormously complicated and extensive systems of information upon which the post-industrial world has become so reliant are, of course, themselves almost completely reliant on computer technologies. This in turn calls for a computer literate population. So far, many millions have attained computer literacy. However, its linguistic and epistemological status are by no means clear. this is due mainly to its newness. At the present time, computer technology is still somewhat novel to most people. It has only really become widely available in the last five to ten years. However, its new affordability has led to an increased acceptance. This increased acceptance has brought with it a heightened level of interest through the general public regarding the capabilities and perceived advantages offered by these machines. As more and more people become computer literate they seem to become less and less patient, more easily agitated, etc. Will any more side-effects become apparent? In ten years time could we witness new syndromes such as 'Post-Windows Stress Disorder'? This might sound far-fetched but I would argue that it is becoming increasingly easy to lose contact with our natural perception of reality if we sit obediently in front of monitors every day. In the alternative reality of the microprocessor, the same rules do not apply. The nature of the medium requires a deconstruction of the thought processes, and what we require is a new perspective on our view of the relationships between blocks of information. Immersed completely in this decontextualised artificial world that in time users can find it very hard to relate properly to the real world around them. An analogy with Marx's analysis of the machine is appropriate. The computer stores not dead labour but dead knowledge. The computer replaces not the

arms and muscles of the worker but his mental functions of memory and calculation, among others. It stands against the worker like his alien essence, dominating the work process. The reversal of priorities Marx saw in the factory whereby the dead (machines) dominate the living (workers) is extended by the computer to the realm of knowledge. Like mechanical machines, the computer shapes the mind of its user; unlike other contrivances it engages the user's consciousness. Its powers seem to enchant users who become absorbed by its capabilities. The line dividing subject and object becomes blurred. Which is the subject, the computer or the individual?

"If Languages have states of health, sick or well, then ours is Manic." (Michael Heim...' The Metaphysics of Virtual Reality'). Infomania is a phenomenon that media-ecologists typically get upset about. Data becomes an eighth plague, 'infomania' retards rather than accelerates wisdom. To them, information is not some new environment into which we will naturally inhabit, rather it is an avalanche bearing down upon us. To Heim, the genuinely existing text surplus is no sign of wealth, but a danger to 'mental capacity'. So what can we do? The computer is now a machine which cannot be turned off. All we can do is recognise our own limitations, beyond which we lose control. To quote John Dewey: *"without control of ourselves, our use of other things is blind"*.

Fear of information overload could be seen as a manifestation of a late 20th century tendency to not allow oneself be guided by extremes. Technology must not be allowed to run wild, a degree of discipline among the colonists of Cyberspace is necessary if we

do not wish to become bogged down in an information swamp where information is so plentiful that it becomes useless. Wisdom does not depend upon how much you know, but how well you understand and your ability to utilise what knowledge you have. This becomes almost impossible if you find yourself not knowing where to begin.

This is why it is necessary to *"preserve the better aspects of pre-digital reality in order to balance the technology that is changing our given reality"*. (M. Heim) This all falls into the realm of the philosopher-technician, who must offer something that the sales managers, market research analysists, and futureologists cannot. And that is *"the conceptual precision needed in order to expand the conceptual basis of technology"*. (M. Heim)

We are talking about a profound shift in the layers of human life and thought. This is an ontological shift, a change in the world under our feet in the whole context in which our knowledge and awareness are rooted. The question here is how much humans can change and still remain human as they enter the Cyberspace of computerised technologies. It may not be possible to turn the machine off, but maybe we can slow it down just enough to stay in control, to use it to enhance our humanity rather than oppress it. Unfortunately, this does not appear to be the course which events are taking.

Soon (by the turn of the century) it is expected that there will be more storage space, i.e. computer memory available than there will be information to fill it. When this happens, the demand for storage space will give way to a demand for information. Once the

databanks are up-to-date they will begin storing information directly at its source. New fresh information will instantly be received by archives with appetites as voracious as their storage capacities are seemingly limitless. After all, when we consider that the production of bulk memories has assumed greater proportions than the combined war industries of the Third Reich and the Allies in 1944, it is easy to see how a data vacuum seems inevitable. Data archivists who have so recently become free from old physical limitations seem to have contracted a form of storage mania. Storage space doubles every year, and at half the price. So now, relieved of the tedious obligation of having to decide which information is worth saving, why not just save it all, just in case.

It would appear that a growing number of organisations are starting projects aimed at collecting and cataloguing everything from culture to asteroids, from DNA patterns to credit records and, indeed, a more sinister application which I shall go into in more detail later, of recording and reviewing telephone conversations. The subject becomes secondary to the fact that it has been recorded or archived.

The mode of information involves the question of language in relation to society. how language defines our powers of conceptualisation and so influence the shape of our experience.

Surveillance, the confessional, psychoanalysis - these are the technologies of power that have their great effect through their linguistic permutations. They involve a flow of information from

the object/individual/social group under scrutiny to the authorities and the collection and storage of this information. The existence of this network and an awareness of its existence by the scrutinised population constitutes the technology of power. Domination here takes the form of a complex articulation of language. When this is considered, it becomes apparent that the latest and perhaps the most complex articulation of language, the 'conversations' between information processing, machines (computers) and the 'conversations' between these machines and their users have an enormous potential for domination and it could be said that they already represent an extremely important component in the 'technology of power' which casts its shadow upon and, in fact, could be said to define the present social order.

The text which chooses to appear on the network instead of on the coffee table, strives for the greatest possible economy of word. Reading pleasure used to be based on an appreciation of authorial style, not just the story lines. The computers response however is to recognises this as static and an obstacle to communication. The electronic readers have all their texts pre-scanned, filtering out added value. For example, there is a 'killfile' that destroys all sources and examples from before a given date; a 'quotation eraser' that gets rid of everything in quotes; the command 'skip interdisciplines' that erases everything except the reader's specialisation; 'create summary' that summarises a text according to the reader's wishes' and 'show method' that shows self-referencial excerpts and takes out all the exercises. What all this amounts to is 'Textual cleansing software' - facilitating the previously mentioned 'decontextualising' tendency - above all

writing on computer must never reach a conclusion; if it did the train of thought which produced it would have to be left out. If we consider how this textual cleansing could be applied to files containing information on individuals it is easy to see how dangerous this might be. Someone or some organisation which used this software on files containing detailed personal information on an individual and decided to take action according to the supposed 'knowledge' gained from such a file (which could be completely misleading and out of context) could have disastrous life-altering implications upon that individual as well as their family, friends, co-workers and conceivably anyone listed in their file as being 'known associates'.

Information can only be converted into knowledge when it is taken in context. What is really important is the relationships and connections between different items of information. Information itself is not knowledge. How we design information, i.e. how it is presented or in what form it takes and how it is manipulated and then applied is fundamental to what it allows us to know. Information technologies and computer storage of data present us with the ability to collect enormous quantities of information. However, this does not automatically give credence to the quality of this information. The potential for digital technology to present information out of context is enormous. This is something which does not seem to be recognised by many people and/or institutions who have become increasingly reliant upon computers for all their information requirements. There would appear to be an assumption, especially on the part of those with little or no understanding of the rudiments of information technologies, that

if it comes from a computer and appears on a screen it must be true. This is an aspect of the notion, among many, of the inevitability of progress in science and technology and that progress is automatically a good thing. Technology carries with it a very strong aura of scientific authority and of truth in much the same way as the printed word was considered by many to the fact in the 15th century, which, as we know, is not the case. The major difference between the printed word and the text which appears on a monitor lies in the fact that printed text has to follow a linear progression, the distinction between author and reader is clear. however, now with text files on a computer, the reader can navigate their own path through the information presented using the interactive nature of the medium. This has the effect of blurring the distinction between author and reader. The whole process is now open to individual interpretation. Although this can be seen as being very beneficial in that it opens up a whole new method of communicating information, it also presents the possibility of once again decontextualising the information obtained which can lead to conclusions being drawn which are not necessarily accurate, although to all intents and purposes they would appear to be perfectly sound and would have an air of factuality. A good example of this phenomenon, and one which substantially questions the prudence of trusting answers that come from a machine has become known as the Ptolemaic Fallacy. A computer model could work smoothly, reproduce experimental results in great detail, even give observations and yet still be totally wrong. eg; we have the historical precedent of the orrery (a clockwork model), circa 1400 built to represent a geocentric universe, like the one the first century astronomer Ptolemy

discrepancies between the simulated universe and the real one. With enough effort we could match the model's accuracy to that of any available telescope, and so we would never detect a failure.

As I have stated earlier, no longer are the individual chunks of information important in the way we develop knowledge through machines, but the relationships between them. In other words, the machine is creating a computer model of the information it received, and those models then determine the way we look at reality. But is it not fair to say that computers de-construct the human context and construct a disembodied machine context, and that this can be seen as being an inherent flaw as regards human decision making akin to the Ptolemaic Fallacy I have just described.

In the United States, the FBI have announced that an encryption chip will go into all phones and computers that they buy. This sounds logical, they wish to preserve their own privacy. But what is their goal in the long run?

> *Every carrier must ensure that its equipment allows for interception of a communication concurrent with the transmission and provide call identifying information to a remote government facility. Manufacturers and support service providers must also assist by developing equipment and software with these capabilities. Providers have four years ... to comply.* (FBI's proposed "Digital Telephony and Privacy Improvement Act, 1994").

This new law would legalise a computerised universal surveillance system on the digital telephone network. Now consider that all

This new law would legalise a computerised universal surveillance system on the digital telephone network. Now consider that all new phone systems in the United States, wired and wireless, will be digital in the next three years.

A very simple and inexpensive way of imposing a degree of total surveillance upon a population would be a government-issue encryption chip in all personal computers and communication devices. Of course, in order for this to be effective the chip would have to be tamper proof, and in fact, the technology to do just that has already been developed at the Sandia National Laboratory, USA. Scientists there have developed an optical sensor that uses a layer of powdered silicon embedded in the chip. This can detect even the slightest intrusion into the chip, which would then automatically send an 'alert' signal down the communication line to an 'interested' party telling them that the chip was being tampered with. In the near future, all encryption hardware and software in the United States will be subject to Federal registration/authorisation. Possession of unauthorised encryption/decryption capability will be punishable as a Federal felony. In other words, if it doesn't have a handy back door for the NSA then it is not legal.

Chapter Two

The hour and the moment of the lists, of the inventories and maniacal enumerations has arrived. For example, there is the world heritage list, 409 sites around the world such as the caves at Lascaux in France, the Pyramids of Egypt, the Taj Mahal, the Grand Canyon and even the Statue of Liberty in New York. These are all sites/monuments which have passed a stringent set of requirements which is necessary in order to be included on this list which has been compiled by the World Heritage Committee, a branch of UNESCO. Its objective is:

> *to define the world-wide natural and cultural heritage and to draw up a list of sites and monuments considered to be of such exceptional interest and such universal value that their protection is the responsibility of all mankind.*

Does this mean that anything not included on this list can go to ruin without having any impact upon world culture? I believe that this process of list-making will extend beyond its present application of archiving historical sites and monuments towards a compulsive urge, spurred on by more and more available memory, to make inventories of everything and everyone.

The temptation to categorise and pigeonhole will always be there and will even be favoured as this would facilitate the list-making process.

With the recent introduction in the United Kingdom of the Criminal Justice Bill, police are now empowered to demand a DNA sample from suspects. These samples are all being catalogued into a national DNA fingerprint register. Taking the form of a computerised database, this will be the first such register in the world. The commissioners and compilers of this database intend it to be a national register, i.e. it would eventually include every citizen. The argument in favour of this claims that it facilitates and greatly increases the accuracy of the police in finding and convicting criminals. This may be true, but it would also facilitate and greatly increase the ability of the police to identify individual citizens and categorise them according to criteria of their choosing, e.g. political affiliation, ethnic grouping, economic class, religion, etc.

In fact, a centralised register such as this has remarkable similarities to plans proposed by the Nazi regime during World War II. As well as this, the real accuracy of this method of identification has been called into question.
In several recent cases both in Scotland and in the United States, false-positive identifications have been made and have led to innocent people serving sentences of up to five years, their convictions being reliant upon inaccurate DNA tests. And these are only the cases which have been discovered. This is yet another, more sinister, example of compulsive list-making, a need to store information, and also an unquestioning (and therefore very dangerous) belief in the absolute truth of science and

technology. Not only has DNA testing been proved fallible, also being debated at the moment is the validity of image enhancement as an accurate source of evidence. This technique relies on the use of a computer to adjust the contrast in the picture. however, this can be very misleading, as shadows can appear to become physical features and physical features can appear to change shape. this sort of evidence has also been used to convict people who were later proved to be innocent. I have given these examples of forensic evidence used to convict innocent people as an illustration of how misleading data can have very real and devastating effects on people's lives and to show that this is not just theory which has no foundations in reality but is, a problem which has no easy solution.

Inaccurate or misleading data which is held on individuals is not confined to forensic evidence or police files. It can be found in the computer files of private companies, local authorities and especially in financial institutions. One example of a blatant abuse of trust and information on private individuals is an advertisement which ran in several newspapers and magazines in California. It gave a freephone number and urged people to call who had trouble getting credit or were in financial difficulty. It gave the impression that by phoning and giving your personal details they could help you out of your difficulties. However, what they were doing was compiling a list of everyone who got in touch with them and selling this information to financial institutions for the purposes of blacklisting these individuals as bad credit risks. Everyone who telephoned was included on this

list, even people who were financially secure, as the fact that they phoned at all, even purely out of interest, meant that they were the sort of person who could possibly become a bad credit risk. The same logic is applied by insurance companies who, for example, include on application forms a section asking if the applicant has ever had a HIV test. This is not to ascertain the result, as the company would not insure anybody who was HIV positive, but rather to determine if this is the sort of person who would need such a test at all, because if you ever had such a test you must be sexually promiscuous regardless of the result and, therefore, a bad risk.

As almost every form of communication, and almost every form of record keeping becomes digitised, the ability to monitor and very quickly assimilate information from diverse sources becomes easier to those who wish to know, i.e. those in power.

The authorities, it would appear, even though they are the greatest hoarders of information, are beginning to set priorities and take drastic measures to curtail unregulated hoarding of information. Authoritive bodies such as Government departments and State military and security organisations have begun to recognise the potential for private individuals and organisations to communicate and store vast amounts of information, through the use of high-tech computer equipment, without the possibility of Government or national security organisations being able to monitor them. An example of steps which have already been taken is the recent banning by the US Government of the continued production of the Clipper Chip (a device which is used

to encrypt data transmitted over phone lines). With the UN at the forefront and the US government catching up, a special commission is currently trying to determine whether or not it would be better to prohibit data compression. This would have the effect of reducing the amount of data which could be stored by existing machines and would also restrict the ease of data transmission.

Why are the impositions of these restrictions seen as something that may be necessary by the powers that be? For a start, is it obvious that these restrictions would not apply to those implementing them, but only to the private population. This is because in recent years the technology employed by the state as a means of surveying/controlling its population has become increasingly available to that population which could potentially use it as an effective counter measure to state surveillance.

When this is considered in the context of electronic surveillance and the gathering of information in databanks on individuals the inherent danger becomes clear.

There are numerous organisation around the world who specialise in information gathering, some on a truly enormous scale. These are inevitably state run organisations, security and intelligence agencies which were set up in the years just after the Second World War and which were kept very busy during the Cold War. However, with the apparent collapse of the Communist bloc, Western intelligence agencies are becoming increasingly concerned with, and devoting more attention to the Pacific Rim

and Middle Eastern states for obvious economic reasons. But, perhaps one area where they are concentrating most attention is upon their own populations. Basically, what has happened is that these organisations have had to re-define their role since the end of the Cold War, and it would appear that they now perceive their new role to include state surveillance of their own people. This is not only aimed at individuals seen as being anti-establishment or subversive but includes everyone, as everyone has the potential to protest.

Physio-political techniques as described by Foucault, and which are mentioned in Chapter I, include police video surveillance in public areas which are aimed at the general public and having the 'Panopticism' effect of intimidating the public. However, specialised state intelligence organisations operate on many other levels. They survey the broader picture of international operations, i.e. surveillance of other countries and their governments, but also much more specifically, of individuals. These individuals could be anyone involved in politics, in business, in protest groups, even in charities or community action organisations. What sets these intelligence organisations apart from the civil police forces is their unaccountability. They are, by nature, secret organisations, and they have to be in order to be effective. However, this means that their potential to seriously infringe the civil liberties and rights to privacy of any individual is huge.

Chapter Three

The National Security Agency (NSA) of the United States is the world's single largest information gatherer. It operates a global network of SIGINT (Signals Intelligence) facilities. these stations are very similar to satellite telecommunications stations around the world, such as the Telecom Eireann earth satellite station of Elfordstown in East Cork. However, what registered Intel Stations send up to communications satellites, the SIGNIT stations, pull down again. This could be described as a form of space-age phone tapping. In the world of international spying and espionage, the traditional human intelligence gatherers have been pushed to the sidelines by Signals Intelligence, or SIGINT. At least 80 per cent of intelligence now obtained by the major Western powers comes not from George Smiley-type figures of spy fiction writers like John le Carre, but from the global network of electronic eavesdropping stations, relay sites, spy satellites and computers run by the United States in co-operation with it intelligence partners. In the words of one commentator: *"Exit Smiley, enter IBM"*. The NSA was established by Harry Truman to co-ordinate and consolidate the individual electronic espionage efforts of the Army, Airforce and Navy. It now commands the largest single budget and generates in return an estimated forty tons of classified documents per day. Its headquarters are situated at Fort George Meade which is equipped with an eleven acre computer complex which is unrivalled in its technological scale

and sophistication. some computers are programmed to break down the communications codes of foreign governments – allies as well as adversaries – while others systematically scan virtually every international telex, telegram, telephone conversation in search of data of interest. The latter do this by watching for key words and can analyse intercepted communications in this fashion at a rate of four million characters per second. In other words, they can read and index a daily newspaper in less than the time it would take the average reader to pronounce the title.

Not least of NSA's achievements has been its ability to conduct its operations outside of public view. Although larger in scale and importance than its sister intelligence organisation, the CIA, for most Americans the National Security Agency does not exist, or is confused with the National Security Council. And that, one assumes, is how the NSA would prefer matters to remain. It was only through the post-Watergate American Congress investigations into the activities of American intelligence agencies in 1975, that a corner of the veil that shrouded the NSA for more than two decades was finally lifted. In the words of Congressman Church:

> *The name (of NSA) is unknown to most Americans ...* (yet it) *is an immense installation. In its task of collecting intelligence by intercepting foreign communications, the NSA employs thousands of people and operates with an enormous budget ... its expansive computer facilities comprise some of the most complex and sophisticated machinery in the world.*

NSA's technology could *"at any time be turned around on the American people"*, Church warned, adding that *"the capacity is there to make tyranny total"*.

During the American Congress investigations, this feature of NSA's activities emerged. The Agency was (is) spying on anti-establishment groups and individuals both at home and abroad. By 1974, the NSA had built up detailed computer dossiers through communications monitoring on some seventy-five thousand American citizens, including former Attorney General Robert Kennedy, civil rights leader Martin Luther King, and anti-Vietnam war campaigners such as Jane Fonda and Dr. Benjamin Spock.

According to the Church committee of the American Congress, NSA's watch list included *"prominent Americans in business, the performing arts and politics, including members of Congress"*. The committee went on to note that:

> *The great majority of names on the* (NSA tapping) *watch list have always been foreign citizens and organisations, who like their American counterparts, are members of radical political groups, from celebrities to ordinary citizens involved in protest against their government.*

The British equivalent of NSA is the GCHQ (Government Communications Headquarters) based in Chelthenham. In January, 1987 the Irish Times reported that Britain's GCHQ regularly intercepts diplomatic radio messages sent to and from Irish embassies. Quoting 'high-level sources', the report claimed that electronic surveillance was particularly intense during the negotiations leading up to the Anglo-Irish Agreement of December 1985. So serious was the situation that all sensitive material concerning the negotiations was either carried to and from London by diplomats or given to Aer Lingus pilots to bring across the Irish sea. Improved relations between Dublin and London

governments since the signing of the Agreement has not meant any lessening in GCHQ's surveillance of Irish radio, telex and telephone messages. The report continued that not only are Irish government communications regularly bugged, those of its citizens are just as closely – and as covertly – monitored.

All of this country's telecommunications with the world at large (with the exception of the Elfordstown satellite station) must first pass through Britain directly under the electronic noses of GCHQ and NSA's British bases. As might be expected, telephone conversations between Britain and all parts of Ireland receive particularly close scrutiny. In October 1982, The Sunday Times revealed that the NSA Menwith Hill station in Yorkshire taps all communications links crossing the Irish Sea and stores much of the information obtained in its computer banks. According to the report, telephone intercepts that may be of value in combating Irish paramilitary activity on the British mainland are passed on to the UK Security Services (MI5).

Duncan Campbell has reported in the New Statesman that Menwith Hill personnel went on full alert immediately after an IRA bomb attack or other paramilitary activity in Britain. The timing is revealing, and it is not the base guards that go on over-time, by the communications analysts. Their job, an NSA official in Washington told Campbell, is to sift through already recorded telephone conversations between Britain and all parts of Ireland in search of clues concerning a forthcoming attack. *"Tape is cheap,"* the official explained, *"storing an hour's calls on a 1,000 line link is simple and would cost less than $100 worth of tape"*.

Along with this periodic blanket surveillance of communications links across the Irish Sea, it would be surprising indeed if the standard NSA watch list procedure is not applied to telephone conversations between Ireland and Britain. That is to say, calls between certain numbers would be intercepted and analysed on a regular or permanent basis. Similarly, Menwith Hill's voice recognition computer systems would be programmed to scan all Irish-British telecommunications links for phone conversations between targeted individuals.

Obvious candidates for such special attention would of course be suspected paramilitaries and subversives, and other politically troublesome individuals and organisations. But, if NSA practice elsewhere is any guide, the Irish-British intercept watch list would, in addition, embrace key establishment figures and decision makers. Any interesting information obtained would in turn be made available to the relevant British/American intelligence, economic and political authorities or perhaps stored on site, in what one former British military officer who visited Menwith Hill described as *"a computer file dossier on European political and trade union leaders"* (New Statesman, July 18, 1980).

Communications between Ireland and the rest of the world are no less vulnerable to clandestine tapping. Menwith Hill is also responsible for intercepting communications from Britain to Scandinavia, continental Europe, Africa and beyond. The task of monitoring transatlantic links between Britain and the Americans falls upon another SIGINT installation – Morwenstow, located on

the cliffs of Sharpnose Point, just north of Bude town in Cornwall. In the words of a former NSA officer:

> There are three satellites over the Atlantic, each capable of transmitting on about 20,000 circuits. There are eight transatlantic cables with about 5,000 circuits. NSA monitors all of these circuits, collects and records the electronic information transmitted, and its computers can pick out the messages it wants by 'key words'. (New Statesman, July 18, 1980).

Morwenstow is a joint British/American base; its twin ninety-seven foot satellite snooping dishes have been nicknamed by insiders as 'Pat' and 'Louis', in honour of former NSA directors. Its taping capacity is believed to include access to transatlantic submarine cables which come ashore at other parts of the Cornish coast. Some of these oceanic cables, and the nearby Goonhill Downs British Telecom earth satellite station, were partly financed by the Irish Department of Post and Telegraphs in return for their use in carrying Ireland's international communications.

It is clear to see that Ireland's internal and international communications networks are completely accessible – as are those of almost every other country – to organisations such as the NSA. This in turn translates into these organisation wielding a degree of power over the individual group, political party or even the government under scrutiny and is an infringement of human rights on a global scale, under the all encompassing, ever flexible excuse of 'national security'.

Conclusion

Apologists and enthusiasts for the further expansion of video surveillance and even more comprehensive systems for personal identification cite the undoubted effectiveness of these systems in the control of criminality. They say " If you are innocent you have nothing to fear ".

In his paper ' A determined effort to explain to a New York audience the secrets of German democracy ' (1979). The German writer, Hans-Magnus Enzenberger, in a chapter titled ' Consent and Erosion ' , says, " But there is another more fundamental reason why it is more difficult to come to grips with the progressive system of social control than with its predecessor. The reason is that it enjoys the passive and in part the active support of the massive majority of our population . "

Referring to the economic success of the Federal Republic as partly responsible for this state of affairs he continues ... " Consequently repression and control take on quite new features. They no longer require - or no longer exclusively require - to appeal to the unconscious, to resentment, racial hatred or chauvinism in order to divert the anger of the oppressed by projection ; instead they direct everyones attention to his own self-interest."

Erzenberger goes on to suggest that the gurus of progressive policing like to generalise from the model of the airport security check - we welcome it in the interests of not being blown up or

hijacked. The large majority of all citizens will accept control measures that offer the maximum security. Thus " The loss of a sacrosanct private sphere is accepted and the surveillance agency can without encountering massive resistance, prepare to store data on an entire population which ' After all has nothing to hide' . "

In the Chapter entitled ' Invigilation of the private sphere ' Erzenberger describes the system in operation in West Germany at the time (1979). "Moreover the use of data by the police reaches far into what are supposedly ' private ' areas informally the booking systems to hotels, car hire firms, airlines, travel agencies, estate agents, pawn brokers, and credit enquiry offices are tapped. All this storage of information is conducted on the principle: record as much as possible never delete anything." the information is centralised at Police Internal Security Headquaters in Weisbaden.

Noting that few contamporary philosophers are prepared to draw up and prepose a model of a future society he suggests that 'a grim sense of humour' might be needed by students of the growing system of control. It would indeed be a bad joke if it were left to the police to work on the 'Great Model' for future society.

"They wish to present us with a new Atlantis of universal internal security, a social democratic Heliopolis, an island fortress for social automats, led and directed by the omniscient and enlightened high priest in Weisbaden (Dr. Herold, Chief of Internal Security).

more laudable dreams of mankind, this 'utopia' will come to a bad end. Presumably it will not be organized protest that will reduce this stronghold but a mightier force - erosion with its four slow irresistable riders called laughter, muddle, accident and entropy."

Written sixteen years ago in Western Germany in the context of the ongoing cold war, Erzenbergers description of the surveillance situation then still bears a strong general resemblance to the situation now. The main differences are that the technology has become more sophisticated and the video camera is now more common in public places.

Foucault, it would appear, hit the mark when he said that "Our society is not one of spectacle, but of surveillance." Surveillance has become intrinsic to the way our society is run. Without it the degree to which the state can implement control would be greatly reduced, and it is not likely that that control will be relinquished.

Questions as to how far the process of surveillance can be allowed to go, can only be decided in the politicaNegal arena. The representitives of civil liberties who pursue these battles against the invasion of individual privacy, will be hard put to keep pace with the developing technology.

I have tried to remain objective in my research for this paper, all the technologies and Government facilities which I have described exist in the real world of the 'here and now'. In doing so I hope I have avoided criticisims of being paranoid or of delving into the realm of science fiction.

have avoided criticisims of being paranoid or of delving into the realm of science fiction.

Bibliography

Mark poster
Foucault, Marxism & History
Polity Press, Cambrige, 1984

Hans-Magnus Erzenberger, *A determined effort to explain to a New York audience the secrets of German democracy*
New Left Review # 118
New Left Review, Oxford, 1979

Phil Patton, *Caught*
Wired, 3.01, 1995

Who's Watching You ? Video Surveillance in Public Places
Briefing No.16
Nat Council for Civil Liberties, London, 1989

Your Right To See Your File
Briefing No.8
Nat Council for Civil Liberties, London, 1987

GCHQ stations and their evesdropping targets
New Scientists, 5 APRIL, 1984

Duncan Campbell, Michael Joseph
The Unsinkable Aircraft Carrier
London, 1984

James Bamford
The Puzzle Palace
Sidgwick & Jackson, London, 1983