SOCIAL POLITICAL DISCOURSE OF THE SURVEILLANCE SOCIETY

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF SOCIAL SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

EGEMEN NİLÜFER YUMURTACI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

IN

THE DEPARTMENT OF SCIENCE AND TECHNOLOGY POLICY STUDIES

SEPTEMBER 2003

Approval of the Graduate School of Social Sciences

_____

Prof. Dr. Sencer Ayata
Director

I certify that this thesis satisfy all the requirements as a thesis for the degree of Master of Science

_____

Assist. Prof. Dr. Erkan Erdil
Head of the Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assoc. Prof. Dr. Mehmet Okyayuz
Supervisor

Examining Committee Members

Prof. Dr. Ahmet İnam _____

Assoc. Prof. Dr. Mehmet Okyayuz _____

Assist. Prof. Dr. Erkan Erdil _____

ABSTRACT

SOCIAL POLITICAL DISCOURSE OF THE SURVEILLANCE SOCIETY

Yumurtacı, Egemen Nilüfer
M.Sc, Department of Science and Technology Policy Studies
Supervisor: Assoc. Prof.Dr. Mehmet Okyayuz

September 2003, 110 pages

This thesis aims to discuss the Surveillance Society discourse, especially in relation with political analysis in a historical framework by means of new technologies. This study also analyzes the use of so-called revolutionary information and telecommunication technologies for data recording and tracking is analyzed, which is used to regulate the order of the system by the power holders. The limits of thought are traced to Foucault and Lyon. To this context an attempt is made to show that surveillance/ monitoring is growing as a result of the developments in information and communication technologies. Dataveillance is being carried out by Internet, ID cards, and bank credit cards. Focus is on awareness as a midway between paranoia and utopic futurism against surveillance suppression.

Keywords: Surveillance Society, Power Holders, Dataveillance, Hacktivism, and Awareness.

ÖZ

GÖZETLEME TOPLUMUNUN SOYAL POLİTİK DURUM ANALİZİ

Yumurtacı, Egemen Nilüfer
Yüksek Lisans, Bilim ve Teknoloji Politikası Çalışmaları Bölümü
Tez Yöneticisi: Doç. Dr. Mehmet Okyayuz

Eylül 2003, 110 sayfa

Bu tezin amacı gözetleme toplumu söylemini tarihi bir çerçeve de politik değerlendirme bağlamında yeni teknolojiler üzerinden tartışmaktadır.Bu çalışma aynı zamanda sözde devrimsel bilgi ve telekomünikasyon teknolojilerinin güç odaklarınca sistemin düzenini korumak adına kullanımını değerlendirir. Çalışma Foucault ve Lyon'un belirlediği düşünsel sınırlar çerçevesinde temellendirilir. Çalışma gözetleme ve izlemenin gelişen bilgi ve iletişim teknolojilerinin sonucu olarak genişlemekte olduğunu ortaya koyma girişimindedir. Verigözetimi Internet kimlik ve kredi kartları tarafından sağlanmaktadır. Tez farkındalığı gözetleme baskısına karşı paranoya ve Ütopik futurizm arasında bir orta yol olarak saptamaktadır.

Anahtar Kelimeler: Gözetleme Toplumu, Güç Odakları, Verigözetim, Hacktivism, ve Farkındalık.

ACKNOWLEDGEMENTS

I want to express my deepest gratitude to Assoc. Prof. Dr. Mehmet Okyayuz for his valuable guidance throughout this study and the opportunity he has given to me for creative thinking. I am also indebted to Prof. Veysel Bozkurt for the support he provided. I want to add my special thanks to David Lyon the author of the main source book written on my subject who has replied my e-mails in a polite and encouraging way. They provided me a great motivation to finish this study.

I wish to express my special thanks to Şeniz Tuncer, Başak Yeşil, Berna Yılmaz, Tennur Baş, Erhan Kurtarır, and Kutay Kence for giving a helping hand when I needed most. I am very thankful for their patience and encouragement.

I want to thank my parents Necibe and Fahri Yumurtacı for being so helpful and thoughtful, and special I want to thank to my brother Mehmet Ali Yumurtacı for his very creative thoughts. They provided the best support throughout this study, with abundance of love. Finally I want to thank to all of my friends whether they are near or far who listened to my sufferings.

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Date Signature

TABLE OF CONTENTS

ABSTRACT ……..iii
ÖZ ……..….. ….iv
ACKNOWLEDGMENTS ……..…. … v
TABLE OF CONTENTS ……. vi
LIST OF TABLES..……... … viii
CHAPTER
1. INTRODUCTION ……..…… 1
2. HISTORICO -THEORETICAL FRAMEWORK …… …. 8
2.1. Explanations of Keywords and Terms ..... … 8
2.1.1. Data …… 9
2.1.2. Information …….. …10
2.1.3. Knowledge ..…… 11
2.1.4. Wisdom ……. . 13
2.1.5. Relationship between Information Hierarchies and Computers…… ... 14
2.2. Attitude towards Technology ……. 16
2.3. Different Theoretical Perspectives for Reading New Technologies 19
2.3.1. Utopianism and Futurism …… 20
2.3.2. Technological Determinism …… 23
2.3.3. Social Constructivism 24
2.3.4. Political Economy …… 25
2.3.5. Postmodernism …… 26
2.4. Political Power via Surveillance Technologies in Historical Background ……..…..26

2.4.1. Social Change …… . 28
2.4.2. Time and Space Independency …… 34
2.4.3. Commodification of Data ……..... 35
2.4.4. Shifting from Discipline Society to Control Society ……... 38
2.4.5. Privacy versus Secrecy …… ….42
3. THE TECHNO-HISTORICAL BACKGROUND OF SURVEILLANCE SOCIETY ……. 44
3.1. From Analog Technologies to Digital Technologies …… 47
3.2. From ARPANET to Internet …… 48
3.3. Intelligence Agencies & Crowd Control Projects …… 55
3.3.1. Echelon and Enfopol …… 56
3.3.2. Carnivore …… 58
3.3.3. Magic Lantern …… 61
4. SURVEILLANCE SOCIETY ……62
4.1. Surveillance Society Debate …….. .62
4.1.1. Globalization as the Supporting Sub-discourse ……..... .68
4.1.2. Focus on Panopticon: Bentham, Orwell, Foucault …… 74
4.1.3. Categories of Surveillance Technologies …… ... 80
4.1.4. New Data-Gathering Technologies and Dataveillance …… …. 83
4.1.5. ID Cards and MERNİS Project in Turkey …… …. .88
4.2. Alternative Attitudes towards Supervision/ Coercion of New Technologies
Impact of the Information Age on Terrorism/
Hacktivism…….. .. 91
4.2.1. Transgression into Systems: Hacking …… … 97
5. CONCLUSION …… 99
REFERENCES ……...105

LIST OF TABLES

TABLE

1. Sources of Resistance to Change …… 29

2. Chronology of Technological Innovations up to Surveillance Technologies……..… 44

3. Distribution of Internet Users (millions)…… 54

CHAPTER 1

INTRODUCTION

Scientific and technological developments that emerged in the last decades brought about a new time period in which a multitude of different acting models have been offered to be implemented within the fields of economy, politics, and society in order to be able to (re)structurize them. On the one hand innovations in bio-technology, on the other hand, overwhelming developments in information and telecommunication technologies aroused. These developments brought about a chain effect in the fields mentioned above, due to the communication channels existing between them. Driven by technological, political, and economic forces remolding of the structures and practices that constitute our symbolic forms, our interpretive frames, and our modes of interaction had caused a transformation in the society. Individuals in the society constitute the daily life within this new framing and forming.

In the context of these developments, which have deep impact on the society, common facts are discussed by social science scholars in a blurred conceptual context. Although, it is claimed that we are experiencing an Information age because of its novelty and transforming characteristics, there are not clear-cut definitions about its meaning. To exemplify some of these definitions which have been used, to describe emerging society with new adjectives we can make a citation from the work of Veysel Bozkurt (Bozkurt,

2000): Knowledge (Peter Drucker), Information (Yohaji Masuda), Post industrial (David Bell), Post-modern (Amittai Etzioni), The Service Class (Ralf Dahrendorf), etc… are all used to explain the society of the 'new' era instead of one another interchangeably, without criticism. Every period of change, which is attempted to be clarified with new concepts by scholars, unwillingly results in a more chaotic context. Instead of discussing the existence of the facts, some concepts such as information age, and surveillance society – in other words, instead of questioning whether or not these concepts really exist - will be taken for granted throughout this study. The focus will be on the concept of *surveillance society*, especially on *dataveillance*. As a matter of fact, electronic surveillance is one of the most important key concepts for the studies carried out on the revolutionary changes observed in science and technology in the 20th century.

The electronic surveillance is not a new subject matter; wiretapping and other types of invasion of confidential messages have been used as espionage agents and intelligence services to control masses throughout the history. However today privacy invasion of ordinary peoples' daily life exploded and the people find themselves under surveillance and control. Although there are different kinds of surveillance techniques our main focus is dataveillance in which we are unwillingly participant of the surveillance exercise. Some of the systems used for dataveillance are as follows data mining, profiling and matching. They are constitution tools of digital individual in the cyberspace. Data profiling, mining systems used with upholding of new technologies, especially Internet, caused serious problems that resulted in subordinates coming face-to-face power holders. Day by day we are becoming digitalized persons as Roger Clarke (1994) named, through barcoding of computerized processes. Predictions tried to be achieved by surveillance technologies attempt to control the mass and regulate the structures to stabilize the order. The power holders try to predict what will happen in society and hoped to control breakdowns at crises. For that reason importance

of awareness by society as being the material of these routine surveillance practices becomes vital today.

This thesis, first and foremost, aims at going beyond mainstream readings of "technological change" and "human progress," which have dominated both popular and academic discussions, particularly in the last couple of decades with the advent of globalization. More particularly, theoretical and practical connections between technological advances and relations of power/domination in society will be explored in an attempt to challenge the power-blind and hence over-optimistic accounts of recent technological developments.

In this respect, the present thesis, by and large, draws on the "surveillance" literature, which examines the different ways in which current technologies, particularly information-based ones, are manipulated by both states and corporate entities to consolidate their hold on the lives of citizens by accessing information about and controlling ever smaller details of their daily lives. The mainstream approaches usually represent the consequences of new technologies for human well being as one of increased security for the population as well as increased consumer satisfaction. At a deeper level, there is a tendency in this literature to associate technological advancements with human progress and attach an essential goodness to technology. These over-optimistic accounts managed to prevail over all others thanks to the ideological dominance of both the New Right and Neo-Liberal discourses, which are pro-status quo discourses *par excellence*, in the last couple of decades.

Approaching the issue of technological change from the perspective of increased surveillance, on the other hand, forces one to go beyond the dominant representations of the issue to reveal the complex power relations at work. To put

it more succinctly, the states, in the name of providing more security to their citizens, are taking advantage of new technologies to augment their power vis-à-vis society. In the same vein, corporations are manipulating human choices, in the name of improving consumer satisfaction, through the same technologies to maximize their profits and hence corporate power at the expense of civil society. Both are able to do this by making use of new technologies as surveillance tools.

Having touched upon the relationship between surveillance and technology, one can identify two types of surveillance: direct and indirect. In the case of direct surveillance, those who are monitored are perfectly aware of the fact that somebody is watching them either that be a prison guard or a company manager. Closed circuit TVs (CCTVs) are a good illustration of the panoptic eye of the observer. In the case of the latter, surveillance is much more concealed and diffused in the sense that those who are kept under surveillance are unwilling participants in the process. In other words, people are not aware of this situation, or despite their awareness, they are almost obliged to involve in the compulsory data sharing process with power holders, such as state, official agencies, multinational corporations, in order to be able to continue their lives.

The rise of indirect surveillance is closely related to the development of information and communication technologies (ICTs), which completely transformed the nature and scope of surveillance. For instance, the World Wide Web, which was in its origins developed for secret military communications during the Cold War, is increasingly used to track personal on-line footprints in the form of electronic data.

Although the surveillance is not a new phenomenon, the difference between the past and our age lies in the ever-growing technological opportunities

for data recording and tracking processes with the aim of surveillance. The cross sharing between different technologies and databases must be taken into account more seriously to comprehend the contradiction between the discourse used to legitimize the use of new technologies and the reality itself: We are not gaining more *freedom and independency,* we are almost losing them.

It is this second type of surveillance, and new technologies associated with it, that this thesis primarily focuses upon. The reason why we have chosen the second type of surveillance can be explained as follows; indirect surveillance is more diffused, unrecognizable, and inescapable and therefore needs to be analyzed, revealed, and highlighted. Direct surveillance is so clear that it needs no explanations, or revealing on the other hand the *awareness* that we mentioned for resisting surveillance coercion becomes more difficult, crucial in the indirect surveillance. In addition to the diagnosis of the problem, there is also an attempt to propose alternatives to the current use of new technologies as tools of social control.

This thesis tries to achieve this second major objective through a careful examination of different attitudes including technophilia and technophobia, and puts forward a third one based on awareness. Technophilia is the attitude of those who unquestioningly embrace technological developments at all costs. Technophobia, on the other hand, refers to a near-paranoiac state of mind that preoccupies itself with the negative aspects of technology; an attitude that at times results in a total denunciation of technological development. The attitude endorsed in this thesis stands somewhere in between technophilia and technophobia. It approaches technology neither in essentially positive nor negative terms. It calls for an awareness of the ways in which information technologies can be manipulated by power-holders in society for purposes of

social domination, and contends that conscious citizens should take advantage of the same technologies to prevent their use as tools of surveillance.

The only way to survive is to gain the power of knowledge. The exercise of power requires information. This transforming period still has a hope within its undefined borders, for individuals to be informed consciously. The blind spots and the weakness of the system can be realized by total awareness and knowledge about the subtext of appropriate discourse. Although paranoiac conspiracy theories seem so relevant today, it is not as catastrophic as these paranoiacs have proclaimed. We must keep our hope alive to human kind and his free will. If there is suppression there will be resistance (Perolle 1996, Foucault 1980). For this reason, we have to question the possibilities of finding the blind spots of the surveillance technologies so as to create the right tools for resistance.

Our study is constructed around questions like: Should we consider surveillance as control and coercion, as resistance, or as somewhere in between; What is the relationship between fictions and aesthetic practices of surveillance and institutions of social control; Are technologies and political systems of surveillance taking on a new importance in contemporary cultures? Can we control the ongoing mechanism of the system by having detailed information about it? Can we control human beings, and predict possibilities of future actions by tracking their personal data? Can we create alternative ways to total suppression of surveillance?

Throughout our study we are going to use relevant examples of surveillance like national ID cards (MERNİS), cookies in Internet used for tracking people by state and multinational corporations for different purposes, and intelligence agencies' intrusion into private information.

The thesis is organized as follows:

In the Introduction the main focus will be on surveillance, and furthermore the underlying reasons are put forward. In the next chapter, some concepts are redefined according to our subject study in order to clarify the thesis. In the recent decades the term information society has become a widely used buzzword for complex social, economic, and institutional changes related to the proliferation of information and communication technologies. In the third chapter the techno-historical background, surveillance technologies, their application fields and the transformation processes, is provided by examples. Chapter four reveals the surveillance society debate, questioning theoretical approaches and attitudes. In the conclusion, after laying the "catastrophic" current situation of the formation of the surveillance society, a possibility of a rather hopeful end point is shown in the sense that people have to be aware and conscious of the fact that they are steadily monitored and controlled by so called developed, new technologies which we name as surveillance.

CHAPTER 2

HISTORICO - THEORETICAL FRAMEWORK

In order to understand the slight difference between the words that are used interchangeably, some of the concepts and the positions of them within the surveillance debate have to be defined to clarify the way we accept and use them. A historical framing can be strengthened with this clarification of the terms. This will help us to analyze the discursive insistence about the goodness of new surveillance technologies, especially for the sake of secrecy and efficiency. For instance, firms claim that surveillance in the workplace is crucial for efficiency but they conceal the fact that they closely monitor the employers to control and restrain, which means privacy invasion.

2.1 Explanations of Keywords and Terms

By creating our conceptualization well established in a social and political context, we should better understand the roles of communication and information technologies in the transformation of the postmodern era, and the surveillance society debate. In this purpose, we will begin to determine some basic concepts, which will help us to work easier on our social and political context of surveillance society.

First of all we will make explanations of some of the concepts used most commonly. These concepts or facts used one instead of another without questioning their exact meaning. Although, every new period faced with new conceptualization for definition of the period, using of these new produced words instead of one another makes the definition of the period more blurred and complex. To clarify what we mean by these words we put this subtitle to explain each of them.

2.1.1 Data

We use the term *information* interchangeably in different meanings in daily language, but there are important differences what we try to mention. We will represent the same facts by pictures, numbers or words. To begin, we will determine what the data is? Specific symbolic or numerical representations of facts about the world are called data. Data are the factors of manipulation stored as input by the computer. Computers are the transformers of the facts from one to another medium in data processing. Validity concept is related with whether if the data are adequately describing the reality what they meant to. Invalidity is due to an error in typing the data or a conceptual mistake. The data are marks, which we left behind us unconsciously for tracing tool of power holders. The term data is going to be used as one of the main sources of surveillance, which is called dataveillance by Roger Clarke (1988). [1]

[1] http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html

2.1.2 Information

Fritz Machlup's (1983) definition for conceptualization of information society is a good abstract material to structure our contextual texture:

> Information is not just one thing. It means different things to those who expound its characteristics, properties, elements, technique, functions, dimension, and connections. Evidently there should be something that all the things called information have in common, but it not easy to find out whether it is much more than the name. If we have failed and are still at sea, it may be our fault: Explorers do not always succeed in learning the language of the natives and their habits of thought (Machlup and Mansfield, 1983:4-5).

Information can be described as organized and interpreted data. Information exemplifies the interaction between facts. As a result of the recent developments in the field of information technologies, computers, organizes, store retrieves relationships between data faster and easier. In short, different kinds of data are matched because of some relationship they had, by computers. Especially this is an important point for information conceptualization, because we used to think -due to the manipulation in information age's myth production- as if information existence equals to computer age. Computers bring out the speed effect for productivity, but the information was an earlier subject than the computer, the history of information can be traced back to cave man's drawings.

Creating information is making new connections among data. In different ways that can be succeed by rearranging the data in meaningful order. Similar data can be used for different information creation. Nonetheless, sometimes foes interpret data in their sake by using the same resources like the following:

In Turkey, the percentage of the youth graduated from university is growing. One scholar can claim that population growth is and parallel to that unemployment growth. However, another one can also claim that the statistics shows improvements in education. Not only opponents use the same data, sometimes one can use the same data to create information for multidimensional purposes, by rearranging the same data resources.

Information technologies are the subtitle of our subject, which aids to create, storage and later analyses of new information material. Here the focus is at the turning point of high information and communication technologies (ICT) into surveillance technologies. In a skeptic reading, we can exaggerate those ICT innovations have been supported for their ability of tracking. This conspiracy theory can be traced back to the percentage of militaristic research and development studies. Nearly all the technological inventions that we used are originated from a military work. Therefore, the disciplinary society can be exemplified in militaristic disciplinary structure. Highly hierarchical structure and chain of command principle makes the military as a perfect model of disciplinary society (Lyon, 1994).

2.1.3 Knowledge

The information is not equal to knowledge; knowledge is one step further in metaphoric digestive system. Knowledge can be defined as understanding after interpreting the information. Giving a meaning to information, for sake of human needs and purposes. People can get information from different sources, but it can be nonsense without evaluation by the persons rationally. Written information involves in formal knowledge, consciously known and built up through procedures. Informal or defined as tacit knowledge, is usually acquired through

experience which is often gained unconsciously and in face-to-face relations. It is difficult to describe and put into words, each has strongly subjective characteristics. To recognize personal aspect of information and knowledge we have to figure out that our knowledge is as mediated by other people as it is by our own experience. "One person's knowledge is made-up of other persons' knowledge and other people's determinations..." (Haywood, 1995).

Although, knowledge is a path for wisdom it can be used in a spiteful manner, which will be caused by lack of wisdom. We can choose to use our growing knowledge to enslave people in ways never dreamed of before de-personalizing them, controlling them by means so carefully selected that they will perhaps never be aware of their loss of personhood. Surveillance Society debate is based on questioning this devilish use of knowledge, against to majority by power holders, in their self-benefit sometimes with coercion, sometimes-unaware participation of individuals. Giving detailed personal information about oneself for a promotion campaign (like telephone numbers, home addresses etc.) can result in unintended consequences, like telephone calls back from companies for advertisement of their new products.

Knowledge is not infallible but limited; it is a societal routine and is relative to both time and place. Knowledge is a matter of societal acceptance. The standards for acceptance are an agreed set of conventions, which must be followed if the knowledge is to be accepted by society. The set of conventions are not arbitrary; they are considered extensively and have historically produced knowledge claims, which have endured the test of time. In any society, there is a myriad of knowledge claims: those that are acknowledged are those, which can be supported by the forces of the better argument. They are an agreed best understanding, which has been produced at a particular point in time. Such

knowledge claims may become unaccepted as further information is produced in the future (Hirschheim, 1991).

Drucker (1993) argues that, the change in the meaning of knowledge over the last two centuries has transformed society and economy. Formal knowledge is now seen as both the personal and economic key resource, replacing the traditional key resources of land, capital and labor. In its new meaning, knowledge is seen as the only meaningful resource, a social and economic utility, and a resource for systematic innovation, while traditional resources are seen as constraints. Knowledge as the key resource rather than as a resource defines the post-capitalist society. "It changes, fundamentally, the structure of society. It creates new social dynamics. It creates new economic dynamics. It creates new politics" (Drucker, 1993).

The importance of knowledge is to be over informed results in disinformation and chaos by knowledge we can choose the necessary information. This will bring us to examine what we really want. Only by knowledge, people can judge the limits of human beings' capabilities. Awareness can be gained by digested knowledge not by being over informed.

2.1.4 Wisdom

Wisdom is inner ability or talent for the best match with situation and right information, in other words insight. Judgment experience improves our capacity to match better. We usually acquire wisdom through long experimental periods. When we talk about wisdom we do not mean not to make any mistakes but learn from the mistakes that we have done. Just mechanical processes of computers

cannot help us to gain wisdom. Being informed by mess of databases one can never reach to shores of wisdom. The surveillance technology can be embedded in the sake of human beings well being, with only that enlightened wisdom (Haywood, 1995).

2.1.5 Relationship between Information Hierarchies and Computers

Human beings interact within a set of information hierarchies. In the hierarchical order of information process, each step can be either data or information by the same time depending on the position, which it takes in signification. As the information gets higher it gets more abstract as the language we use. Computer's high-level languages are similar to the daily abstractions of language, serves for programmers. An advanced system of information process enables users to make functional structures of relations among different information levels. As the level of abstraction gets higher details of the data can be lost but at the same time relevant information is conserved.

There is another type of information hierarchy at cyberspace, which is called metalanguage; they provide a standard set for other language's formal description. Specifically HTML (hyper text markup language) is a subset of SGML (standard generalized markup language) meta-language. This hypertexts enhancement made it troublesome, for users to understand and catch what is going on, and where the necessary data located in the computer. As the networks of information get more complex, people convinced that there is really a huge shift in the production of information. Here, we will claim that complex, patterns of information creation helps to persuade people that they are experiencing a revolution which they can not involve directly in creating, or sharing and controlling the explosive growth of information.

In fact, we can focus on the culture at that point, which distinguishes human beings knowledge compared to other species. Human beings learn how to act, rather than having genetically establishments. Whenever the societies get more complex and developed, individuals start to accumulate information, as an external extension part of their brain, in the form of common culture. The culture is consisted of information about different subjects established in time, which shapes social structure and at the same time shaped by it. Language, beliefs, traditions, ideas are all included in that formation period (Perrolle, 1996).[2]

The units of cultural information are the symbols. To understand how we are directed for acceptance of a claim, a truth, we have to examine the symbols and codes through which we are informed, and controlled by power. In historical evolution of the society, the power was in the hands of landlords at the period of agriculture, then the power transferred to the capital owners. In the age of knowledge owners of information resources use these codes, though the power is gained by production of information. Derrida (Sarup, 1993) indicated the age we live in, is more symbolic then the ages before, codes became overwhelmed. The image production is made with generally accepted codes of popular culture. The realm of culture became an industrial market as defined by Adorno (Sarup, 1993) and his followers. In postmodern era the coding and decoding concepts became popular, so that when we deal with information society codex, discourse analysis becomes inevitable (Sarup, 1993).

We will identify important themes that weave through the literature, and track the changes in our conceptualization of the surveillance society. After taking stock of the literature on the information age, we will try to understand when, where, and how the information society term actually turned into surveillance

[2] http://www.ccs.neu.edu/home/perrolle/book/Word Sworth Publishing company new material 96/97/98

society and what forces are behind the societal transformations we are currently witnessing, how we begin to turn into *digital persona* (Clarke, 1988)[3] and been accepted as data by power holders.

2.2 Attitude towards Technology

We can classify two attitudes towards accepting technological innovations, which can shape an integrated framework covering all the studies about the subject. One is more positive about its role, which can be called either technophilia/telephilia or optimism, the other is more negative technophobia/telephobia or pessimism. Both technophilia and technophobia are creating an ever-growing gap. By the insiders -the developers and users of technology- a politically motivated, constructive critique could and should take place, within that gap, awareness has to be provoked as the midway to understand surveillance. Dordick and Wang describe these differing attitudes as below:

Technophilia represents optimistic view of the use of technological developments, branded with an obsession with the love of technology that is believed to be the solution and the means to improve human performance in every kind of activity in life. This view glorifies the role of technology in the developments of various daily tasks. Machines would offer a more convenient way of life, being present in people's life under people's control. Optimists, like technological utopians, believe that new technological developments can dramatically enhance the educational process, bringing about more educated people together with easier access to education. For example, according to the optimists, people will be freed from traffic jams and air pollution, since they will have the opportunity to work in their homes thanks to the PCs and Internet. As a result, more time will be allowed for creative work and spiritual cultivation.

[3] http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html

Moreover, broad access to information will help bring about participatory democracy and a perfect market, in which liberal ideals will be realized. In this context, technology is only a tool which is invented for human progress and which will be humanized under man's control (Dordick and Wang, 1993).

On the other hand, technophobiacs who has a pessimistic view, believe that there are no major structural changes to justify a claim for a historical or social discontinuity. Technology is considered as an evil element that plunges humankind into a more dehumanized world, not recognizing any benefit that it might bring to our lives. According to this view, Information Society is doomed by alienation where technology is an instrument of disconnection that isolates human beings from reality. Technophobia argues that new information technologies such as PCs and Internet not only prevent people from establishing real relationships, but they also can destroy social relations that have been already established, which both would result in nothing but human alienation. Surveillance by the bureaucracy will only revive tiresome memories of the industrial age. They see the coming of a dark age where information and information technology only serve to benefit the rich, such as multinational giants, for more profit exploitation as an ideological reproduction tool (Dordick and Wang, 1993).

Through our work when we talk about surveillance our tendency will seem so technophobic, but we are not choosing to be as pessimistic and hopeless as they are. Naturally, if society is defined by surveillance adjective, our inclinations in this study can be seem more likely to be technophobic then technophilic. The society is popularly defined with a new adjective, ***surveillance.*** We will be dealing with surveillance as one of negative the results of the technological developments, which affect social structure. The rise in highly developed recording and tracking technologies like CCTV, satellites, bar coded ID cards, credit cards, biometrics,

Facial Recognition Systems, GPRS systems, Internet etc… had caused this definition. There are different attitudes toward these improvements in ICT and surveillance technologies. One of them is ignorance, the other is paranoia, and the third one is to consider technology as the only determinant of future utopic heaven. The former is beyond our focus, because to discuss the solutions of surveillance suppression, first of all, we have to handle with the group of people who accept the problematic. The second group is technophobics and the third is technophilics. Our attitude can be defined as hybrid; we are neither paranoiac nor future utopist.

There are two different approaches according two different attitudes about the change period also, either claimed the changes in society were a result of technological improvements, or the social changes were caused technological innovations and improvements. The industrial society accepted as a consequence of the new revolutionary technological improvements. The tendency about information society debate points that; it is another revolutionary change via technological innovations of information and communication subjects (these views can be categorized under techno-determinism). Society and culture never remain transfixed to any one point. There is a dialectical interaction between social relations and technological innovations. Politics, economics, technology and society are always in flux in relation to each other, creating a whole that continues to change. We are choosing to be critical and cautious about the *change* concept used in the name of revolution and improvement. Further information about the social change is given under the subtitle of political power via surveillance technologies in historical background.

2.3 Different Theoretical Perspectives for Reading New Technologies

Mainly we will define four main modernist approaches to understand the relationship between society and technology. In addition, we will emphasize the postmodernist, poststructuralist approach, which is more critical and recent. These approaches are used to understand different interpretations of cyberspace as the background of the surveillance discourse (Kitchin, 1998). William Gibson shaped cyberspace concept in his famous book Neucramancer (Gibson, 1984) then the concept was highly accepted and used in different textual readings of society, by scholars with different tendencies and interpretations.

The discussions on technology are diversified according to different approaches of the scholars. Reinecke (1984) distinguishes between the "techno-boosters"--people like Micheal Zey (1994) and often the government, media and business, who embrace Enlightenment discourse and all its promises enthusiastically, pressing onward to liberation in a mythical techno-city. There are the "techno-pragmatists," people like Hellman (1976) who promote "coping" and "adjusting" to technological changes; for them, technology is neutral, and can be used for good or for ill. Finally, there are the "techno-skeptics," like Jacques Elull, who declare Enlightenment ideals to be a fake, and technology to be inherently imperialistic and alienating.

We perceive that while any technological innovation does bring inevitable complementary social changes, these changes has the possibility to be good, and if they are not, they can be challenged by individuals in the course of decision making in everyday life, and by unions, the law, the academy, and lobby groups, and high skilled, well organized anti-surveillance groups. Technology shapes

society, but society can also shape technology, even as technology leads *brave new world*s. Technology is not neutral, but neither is it intrinsically alienating or liberating.

Since the mainstream discourse legitimizes the existing condition of surveillance technologies, a language that challenges the logic of rationality is needed in order to give words to our alienation, the struggle for better worlds. These four main theoretical approaches take technology from different viewpoints. Our study is more likely to be critical all over them.[4]

2.3.1 Utopianism and Futurism

Utopists and futurists try to foresee how technological innovations will affect the society of the future. The "future" in the modern West has traditionally been the special responsibility of people called "futurists" and of a specialized form of social analysis called "futurism". Since one cannot actually know what the future holds, it is imagined by scientists, policy makers, social critics, science fiction writers, and utopian dreamers must be understood as "social constructers" who reveal much more about the present to predict about the shape of things to come, so we have to appreciate the future to understand the present. The general ideology is that all of our problems will be subject to technological solutions. Roszak (1994) explains utopians in two different type a reversionist who seeks a preindustrial life style, or a Tecnophilies seeking a highly well- designed urban industrial living, new order of technology and science. Many of the utopians imagined a picture of future within the words of past, technology could be defined as new framing for old tastes. They hope that technology can solve the problems of past and can create a heavenly free world in future. This can be seen as a

[4] http://spartan.ac.brocku.ca/~pschuurm/thesis/chapter2.html

resistance to the crisis of capitalism, poor conditions of human beings, inequality of wealth, etc. The future as a possibility has the chance for a better world establishment; the main supporter seems to be technology. These futuristic utopias are wishful thinking; at worst, they are misguided efforts at engineering social reality.

The futurist view is inevitably utopian, because of its unprecedented characteristic. Moreover, the precise terms in which new technologies and other future miracles will solve social and ecological problems are never actually addressed; rather, the solution is magical, insofar as the only appearance of such technologies is enough. From this point of view, we can claim that it looks like a heaven image of the religions. In another world construction where all problems will end and the main actor accepted for this revolution is technology. Winner (1992) calls "mythinformation" as such a wonderful world in the guidance of computers that is dreamed by the futurist. The inevitable power of computers at that mystification level is also being covered in another theoretical approach, technological determinism. Also there are two different tendencies in futurism that was figured out by Carey (1989)[5]:

The first of them are conservatist futurists, conservative futurists are those who believe that technology changes, but that social, political, economic and cultural arrangements should remain the same. Power remains concentrated in old aristocratic elites, or in new scientific or technocratic elites. We can give 19th century futurist writers as an example to those conservative futurists, who imagined the future as an extension of the British Empire; information society advocates, such as Daniel Bell, George Gilder, and Alvin Toffler.

[5] http://www..wlu.ca/ wwwblack/cS400/fall02/October8.html

The second ones are progressive futurists, who were variously anarchist, socialist, feminist, etc., believed that technological and social change must occur simultaneously. Power is decentralized, and harmony achieved between technological development and health of the environment. Progressive futurists often dreamed of a future democratic system in which technology would allow citizens to actively and directly participate in governance. Examples of progressive futurists are, Patrick Geddes, Lewis Mumford, and John Dewey.

The most optimistic views of the future come from such as Alvin Toffler (*The Third Wave*), John Naisbitt (*Megatrends*), Grant Fjermedal (*The Tomorrow Makers*), Harry Stine (*The Hopeful Future*) and Eric Drexler (*Engines of Creation*). All of these are willing to foresee many new and better potential worlds resulting from current and projected technologies (Carey, 1989).

The earthly heaven was defined by the leading of technology, future plots created as a result of the problems faced with. The world was in a transformation period and crisis made people hopeless, after Second World War people begun to dream about a better world. The subject of the "future" was largely absent from academic and public debates in the 1950s and indeed through much of the early 20th century. This was changed significantly in the 1960s, at which point Western society "discovered the future". The 1960s are the place where the future became such an interesting topic to media and social critics, to government and business, to policy makers, etc. for that reason the futuristic utopias become popular to read and interpreted. We have to be awake when a new world order is supplied as a heaven resulted from new technologies; a utopia where all sorts of weakness are no more exists. The technologic determinist future story depends on myth of leaving behind the weak points of the system by improvements in technology.

The legitimization of the system using surveillance technologies is made under the belief of security for future utopia with discourse used by power authorities. Media manipulation is one of the main tools served for this discourse creation. Another is rising law enforcements on human rights and freedom which is splashed after 11th September event in USA like Patriot Act signed at October 2001, and anti-terror regulations given more authority of power for state control. The “Patriot" Act passed by the panicked Congress by an overnight revision of the nation's surveillance laws that vastly expanded the government's authority to spy on its own citizens and reduced checks and balances on those powers such as judicial oversight (Lyon, 2001).

2.3.2 Technological Determinism

Technological determinism argues that the social, political, cultural and economic aspects of our lives are determined by technology. The existence of technological innovations is independent from social events. On the contrary, they shape the society, the way of our livings. According to the independence of technology, the society becomes dependent and passive. According to Karl Marx the engine of the history was class struggle, McLuhan (1964) changed that citation into the engine of the history was engine, the technological change, especially new communication technologies, seen as the main force behind human history.[6]

The main problem here is the assumption of these views as separated, they are mutually connected with each other and interpretations have to be made within that interaction. The determinists subject is not how society can learn to insert, adopt technology into their life rather how technology can be changed and shaped

[6] http://www.acmi.net.au/AIC/phd4600.html

for society's benefits. Penley and Ross stated an attitude against the belief of enslavement of human by technology, as cited below in Kitchin's Cyberspace:

> Technologies are not repressively foisted onto passive populations, any more than the power to realize their repressive potential is the hands of conspiring few. They are developed at any one time and placed in accord with a complex set of existing rules or rational procedures, institutional histories, technical possibilities, and last but not least, popular desires. All kinds of cultural negotiations are necessary to prepare the way for new technologies, many of which are not particularly useful or successful.

Internet can be a good example for that, at the beginning it was a reaction to Soviet technical advancements and called as ARPANET. In time using practices turned it into a medium of communication and information center. The Internet has become an integral, ubiquitous part of everyday life in many social domains and international contexts. Espionage tools used in movies for eavesdropping, monitoring became popular goods and sold at small spy shops. Facial recognition system was designed for facial expressions capture and analyses, but then it turned into tracking of criminals and potential criminals by recording their faces as data and matches them with police records. Today at the airports there are lots of CCTV and FRS tools. The potential of racism upraises. A close observation in practice after the 11th September against to Third World Country originated people and Muslims can be given as an example of those racist tendencies which is against to human rights caused by using of FRS.[7]

2.3.3 Social Constructivism

Social constructivism arguments are based on the thoughts of society and technology is embedded and cannot be separated. The one who is against technological determinism constructed social constructivism. Escobar (1994)

[7] http://www.notbored.org/face-recognition-software.html

describes the general belief about the relation between society and technology as "Technology systems are regulated according to flexible techno-social arrangements, which within certain structural constraints constitute social closure around concrete developments".

The cyberspace is understood as a social process of culture, in the name of social construction. Alternative place of public space is being constructed as cyberspace, by the new technological developments that improved abilities of society. Social constructivism refuses the social determinist ideas, which structures of capitalism and the power of political economic forces control how cyberspace has and will grow. The main focus for us is the possibility of surveillance in Internet, which cannot be separated from its panoptic characteristic. Although it was presented as a space of freedom, it is turned into an *iron cage* (Weber) of surveillance, which benefits for state and multinational corporations market research.

2.3.4 Political Economy

Political economists like social constructivist claim that technologies are dependent on society and they must be interpreted in the relationship with society. Moreover they suggest that, the relationship associated political, economic and social relations, which is embedded in capitalism. The relationship between technology and society exists in capitalist modes of production. This approach is focusing upon the relationship that lies in capitalist power and their changing dynamics. Although this is an important approach involved with surveillance and new technologies it is beyond the scope of our study.

2.3.5 Postmodernism

The concepts above are modernist views but postmodernism resist the grand theories of society and social knowledge which seeks to reveal universal truths and meaning through Meta discourse contrary to modernists. Here the postmodernity refers to developing an attitude towards theories, knowledge, and communication under the affect of new technologies. Knowledge is being reconstructed. The postmodern knowledge society is an alternative to modernity. They claim that traditional conceptions are being altered. The new era is reconstruction of the interfaces with ICTs leading.

Despite of the fact that, we cannot ignore the influence of technology in recent changes in society we have to be very sensitive about the discourse, different approaches highlight different face of the developments. These developments in information technology are claimed to be revolutionary innovations that will thrust societies and nations toward renewed economic growth, new modes of political participation, and a rejuvenated sense of community. The role of human being becomes very fateful, the power and authority must be gained back. The inventor and user of technology is one and only actor who can choose to be enslaved or master.

2.4 Historical Background of Political Power based on Surveillance Technologies

We have to look at historical background of the facts to clarify the ongoing procedures. When we talk about ICT, usually we are talking about Internet and other networks established in relation with it. The enormous spread out of Internet

happened at last decade has resulted in a stronger supervision of power authorities over ordinary citizens by databases creation at every part of everyday life.

During the last decades, some of the social scientists have claimed that the main feature of the industrial society has been changed in highly developed countries like USA or Japan. Moreover, they argue that this change has come up as a result of significant technological developments in the following two sectors: the telecommunications and information. There is disagreement among the scholars on the formulization of the new age. These conflicts can be observed especially in the effects of information technologies on cultural values. For example, Weizenbaum (1976) claims that the more important computer produced data becomes, the more we will fall apart from our cultural traditions, contrary to Daniel Bell's location of information process as a support for cultural improvement. Data becomes a good in the markets through the commodification process, which is necessary for information production. The capitalists, especially in developed countries, which are moving into an information society, recognize this new tool of making fortune. They start to record and produce data as a good for markets. Not only does it serve as a tool for profit maximization, but it also acts as a controlling and tracing mechanism. All social relations have economic backgrounds besides the historical ones. For centuries, states have recorded data other than profit maximization: to control and to trace. Governments hope to identify or eliminate system failures by collecting and recording data about its citizens. Although it is still a speculation which cannot be proved by concrete evidence, it is argued by certain circles that personal records of citizens are being sold to companies by state, or vice versa. If this speculation proves to be true, the possible results would be beyond our imagination.

The two polar systems worked at the time of cold war. Third world countries affected by west or the east side superiors. The *new order* ideologically

divides the world into west and east. In addition, developed and underdeveloped division was built between the north and south. The frame was fragmented and the crisis of capitalism emerged at the face of Oil, at seventies. The scarcity problem been discussed, the strategies of environmentalist tendencies flourished. Then, the cover period of the crisis yield to new technological developments. In the long run, those developments resulted in a new era. The society, in which those changes were happening, started to change also. After 1960s foreseen by some of the scholars and debates of information society subject, became popular. At the last decade with other concepts like new world order, postmodernism and globalization *information society* became one of the most spoken concepts, amazingly usually in a speculative structure.

2.4.1 Social Change

The only unchanged truth is everything will change someday is an anonymous definition about change. Every component of human's culture is subject to change. The change sometimes happens as a natural progress without notice and action of man. In spite of the fact that improvement in new technologies is obvious, the matter lays at the degree of the change. In order that the revolutionary character of the age must be questioned instead of taking granted as said so. In England, Rosenbrock (1990) and his friends argues that the main difference between the industrial and information is not a matter of qualifications but a matter of degree. The change was also laying in industrial society' core. The institutions of industrial society are still existing they are partly reformed and rejuvenated (Bozkurt, 2000: 22).

The change always is either opposed or supported with different interest groups in the society. Confrontation of change differentiates from immediate

acceptance to total rejection. There are many forces in any society, which causes resistance to change. Lauda (1971) categorized them as ideas and norms as in the table below:

Table 1: Sources of Resistance to Change

Ideas	**Norms**
Religious doctrine	Common law
Superstition	Statues
Stereotypes	Mores
Myths	Customs
Misconceptions	Folkways
Ignorance	Group pressure
Values	
Fear	

Source: The Complications of Change Donald P.Lauda pg: 264

These non-material components of our culture play the leading role for resistance to change. For example one can refuse to use Internet because of surveillance paranoia (fear), or ignorance of its usage. Acceptance of change depends on the degree of humans' ability to adjust. If the society is strongly dependent on the factors above, the acceptance of the changes will be more difficult too.

Today the difference is the high speed of change that is caused by the technological developments. The speed increased due to the convergence of information and communication technologies. However the technology must not seen the only determiner but one of the causes of the change in social structures.

David Lyon (1994) claims when we talk about technologies impacts on society it means as if they are two independent entities. Emphasizing only technological side or vice versa is a result of false way of thinking. We have to think technological change in a broader context as a social activity, which has political, economic and cultural dimensions. Ability to adapt new technologies affects all these dimensions. Despite of the fact that we have to avoid from being technological determinist, we must not ignore its transforming capacity of these entities.

Indeed, the ability or inability of societies to master technology, and particularly technologies that are strategically decisive in each historical period, largely shapes their destiny, to the point where we could say that while technology *per se* does not determine historical evolution and social change, technology (or the lack of it) embodies the capacity of societies to transform themselves, as well as the uses to which societies, always in a conflictive process, decide to put their technological potential.

There are times when the entrenchment of vested interests hinders all progress. The change adaptation will not be equal in different societies. To say that the differences that exist today in various cultures are never to change, and that *the clash of cultures (Huntington)* is therefore inevitable, will only produce two unfortunate choices; to push others away as completely alien, or to force one's own values onto the other. However, many of the ongoing debates regarding value differences, especially differences between the West and Asia, tend to neglect historical evolution and geographic diversity of values. These arguments look only at the present situation, so appear "static" and superficial. As a result the history is full of the stories of powerful dominants repression over other institutions (Castells, 1996). What must be retained for the understanding of the relationship between technology and society is that the role of the state, by either

stalling, unleashing, or leading technological innovation, is a decisive factor in the overall process, as it expresses and organizes the social and cultural forces that dominate a given space and time. To a large extent, technology expresses the ability of a society to thrust itself into technological mastery through the institutions of society, including the state (Castells, 1996). A powerful nation state has a strong role on regulations of technology and its impact on society. The discourse as Foucault claimed is an ideological tool created by power holders who controls entities of information.

The power elite of late capital for much the same ends have reinvented the archaic model of power distribution and predatory strategy. Its reinvention is predicated upon the technological opening of cyberspace, where speed/absence and inertia/presence collide in hyperreality. The archaic model of nomadic power, once a means to an unstable empire, has evolved into a sustainable means of domination. In a state of double signification, the contemporary society of nomads becomes both a diffuse power field without location, and a fixed sight machine appearing as spectacle. The former privilege allows for the appearance of global economy, while the latter acts as a garrison in various territories, maintaining the order of the commodity with an ideology specific to the given area.[8]

Social change theories are to some extend related with history. For this reason the new technologies development cannot be separated from the historical background. Some of the scholars such as Rosenbrock (1990) as we mentioned before thinks that so called ICT revolution was rooted in industrial revolution. This idea can be find its origins at Social Darwinist theorization. To call an evolution is preferred for recent developments. Then the main paradigmatic shift, which has been caused by new technologies, becomes irrelevant opposite to some of the scholars assertion.

[8] http://transcriptions.english.ucsb.edu/archive/courses/liu/english236/materials/class20notes.html

According to Castells (1996, p. 5) the author of the famous trilogy written about information age, claims that social changes are inseparable from the changes in the technological infrastructure through which many of the activities are carried out, "since technology *is* society and society cannot be understood or represented without its technological tools" Social changes and technological changes are intimately related. Castells theorizes their interaction in the following way: “A society produces its goods and services in specific social relationships– the *modes of production*. Since the industrial revolution, the prevalent mode of production in Western societies has been capitalism, embodied in a wide range of historically and geographically specific institutions to create and distribute profit. The *modes of development*, on the other hand, "are the technological arrangements through which labor acts upon matter to generate the product, ultimately determining the level and the quality of the surplus" (Castells, 1996).

Some of the pioneers of the revolutionary change and believers of a heaven like future are Utopic Futurists, and Third Wave Theorists (Yohaji Masuda, Alvin Toffler) according to them the technology can be described as good because it responds the needs of human beings, and improves life quality. This is related with pragmatist understandings of West. In addition to that technology in general, Internet in particular is defined as freeing toy of capitalism, because by its innovation we are less time and space dependent and accessibility to information is easier then ever before. When these optimists were asked about the side effects of these technologies like privacy invasion or surveillance, they claim that it is necessary for the security of the individual as well as the security of the nation, in other words, their understanding of freedom is not affected by these kind of problems. Moreover there is no need to be tracked if everyone behaves as a ‘good citizen’. On the other hand, the people who are cautious about the new technological realm, bases their objections on the same problems. According to persuasion layer of their claims, these people can be named as skeptical, paranoiac or ‘conspiracy theorist’. They assert for new technologies the

higher capacity they gain for creating and processing information the higher they have surveillance capabilities. Moreover, information technologies are not just providing us information but providing 'others' our data/information. This brings in particular jeopardize of individual privacy in general the control of society. That the aim of developing and investing in these technologies was to control the society can be taken into consideration as the severest of the claims. According to this claim, the leading roles in surveillance of the society belong to the state and the firms with different intentions (Lyon, 1994).

All of these discussions need more than introductory knowledge on how the new technologies work. In conclusion we are going to talk about being aware and well equipped by knowledge can only help us to interpret how true is the conspiracy theories. And then awareness about the realm leads us for creating alternative attitudes and finding blind spots, if any. The tendency to be rationally aware of the world is a necessary precondition for being able to detect change and social change is directly related with rational knowledge. The growth of rational knowledge comes from both a reaction to the Crisis of Control and at the same time being a cause of it. It is a reaction because rationalization is essentially the organization of information, in order to simplify and hence control. It is again, a cause of it because the increase in energy utilization in the production, distribution and consumption process is a direct result of the rational capitalistic methods of production, in which the speed of the utilization of energy gave rise to the Crisis of Control that Beniger (1986) proposed, will further explained in our work.

2.4.2 Time and Space Dependency

To understand the highlighting in the last decade about time and space we have to be aware of their creation first, the boundaries of time and space created for restriction of individuals. Today the independence from these boundaries are being sold beside Internet facilities.*The mainstream discourses on the revolution of information and communication technologies* stress the novelties they have brought about, focusing especially on the liberation of human beings from the restrictions of time and space. The most sparkling exemplification of this rhetoric is bloomed in the concept of Internet. The time and space firstly used fort capitalistic purposes to restrict people now it is proclaimed that we are becoming independent than their limitations. Moreover, Allon in the conference made at Italy in November 2001 on general topic of Spacing and Timing talks about the time and spacing concepts as we cited below:

> The growth of global information networks, the wide-spread adaptation of personal computers and their related networks of everyday communication, along with the pervasive reach of digital technologies in general, have led to further spatial and temporal displacements and dislocations. There is, within this integrated world, a new global arena characterized by a relentless mobility (of commodities, capital, information and labor), by fluid modes of circulation, and also experiences of abstractions and similitude. And overlaid upon the physical landscape is the 'virtual', 'extraterritorial' geography of information technologies, electronic media, satellite footprints and global space they weave together, a space which, without relations of actual co-presence, functions as a skein of connections of presence and absence, of instantaneous communication and absolute proximity, of immediate connections between local places and distant events and between near and far. Images and rhetoric now abound of a world integrated and interconnected through technology and large scale media institutions, of a new communications geography defined by vectors, movement and flows, and of space 'annihilated' once and for all by high speed transportation technologies and instantaneous delivery of information. Traditional spatial and temporal coordinates that

> hitherto afforded a means of orientation and location have, this rhetoric suggests, collapsed and distance has finally overcome.[9]

2.4.3 Commodification of Data

It is said, that the percentage of people who are better off in the material sense today is higher than at any time in the human history before. According to the statistics the poor are not so poor as they once were, and the world could probably feed its entire people. The result is not as optimistic as the statistics tried to persuade us. Set apart from political struggles and power battles, this could be the truth, but economic and technological realities are not as separated and independent from other variables such as social conflicts and power relations.

In Western nations, ordinary citizens control their living space, can buy any kind of basic food and have several modern apparatuses that do more work than a dozen of slaves. Moreover, their leisure time is abundant, and entertainment industries are serving for them. This fact lies in the heart of the main discourse used to legitimize ongoing developments in technology. From this point of view, can human beings be considered luckier than cave men depending on the claim that we are better off?

Against this claim, there are inequalities, even in wealthy nations, the gap between the rich and the poor is great, and there are homeless people even in the most prosperous countries. There is also still a deep abyss between the rich and poor nations. On the other hand, in total framing technology has improved almost everyone's standard of living, and few would care to return to the days of poor

[9] http://www.emp.uc3m.es/~quattron/conference/papers/Allon.pdf

nutrition, no medical care, high infant mortality and low average of life span. In the end, relatively, we are all benefiting from technological developments.

When we are not aware of the subtext of the system we would think as if the only production of current times is, *information*. Information and knowledge were not as highlighted as today for production of capital. The knowledge- the quality and description can be doubtful about the edge between knowledge, information and data- is living its golden age. The knowledge set as a precondition of creation of capital by Alvin Gouldner (1979). Knowledge is equally a part of what we call culture, he suggests that '*the emerging concepts of "culture and "capital" are Siamese twins, joined at the back: culture was capital generalized, capital was culture privatized*' (Gouldner 1979, p 25).

As we cited before, Weizenbaum (1976) claims, as computer produced data becomes more important we will fall apart from our cultural traditions. As the commodification of data that is necessary for information processes, it becomes a market good. The capitalists, especially in developed countries, which are moving into an information society, recognized this new tool of fortune. They started to record and produce data as a good for the market. The state was doing the recording data for centuries for another purpose, controlling and tracing. The system failures could be figured out or erased by this collecting of data about individuals.

There was inadequate discussion of the new commercial databases and implications of the commercialization of information in terms of who can and cannot afford access to expensive databases and how oppositional databases can be used to provide surveillance of corporate and government corruption, and thus be used to promote social criticism and change. Indeed, access to and use of

information will be a crucial feature of the construction of the future. On one hand, corporate control and the commercialization of data bases threatens to increase the power of the wealthy and the state that control data bases, thus increasing the potential for expanded corporate and state power and class division. On the other hand, the computerization of society decentralizes information and gives citizens and oppositional groups the ability to circulate critical information about the government and corporations. How the information revolution will play itself out and what policies government will develop over privacy and surveillance will be among the great adventures of the foreseeable future and the collection under review provides an occasion to reflect upon the futures and choices that currently confront us.

Orwell's Big Brother seems almost unusual compared to these contemporary privacy threats; Big Brother is, after all, the state, and the resource of the threat was clear. In recent years, corporations, organizations and individuals became capable about reaching to our recorded personal data and buying habits, in ways we are only faintly aware of. The threat source became vague.

Life under totalitarian regimes because of their coercion and thought control, and the entry of the state as representative of the "community" into most aspects of private life, is changed in modern state. Surveillance technology's capabilities makes the edges blurred and coercion is not as clear as in totalitarian regimes. Usually we are not aware of the curiosity of the threat. Individual is *unwillingly participating* in surveillance action. Surveillance technology frames the contours of the system of corporate dominance that is changing the relationship between public and private life in potentially radical ways. It is harder at that point to see the systems of power and the potentials for abuse that are part of our daily lives. It is an issue of power and of avoiding assigned power to forces that will use it coercively.

The information sphere has become a battlefield of power/control and capital. As it is drawn by Druckrey[10] an "increasingly dematerialized public sphere" in which conception of self and privacy, distinction between public and private spheres of communication and distribution of time are more transparent and frosted at the same. As Burgess (1994)[11] puts it:

> Where once the earth itself provided the most tangible and fundamental point of reference for human activity and human meaning, the rise of information technology and the change in the status of information itself as a completely dominant commodity, detaches inherent value from the earth… Information technologies create and introduce into exchange commodities that are de-materialized… Information has in itself no use value. It exists to be exchanged, to change form.

To understand those huge changes resulted from developments in ICT as said so, we have to check, in an evolutionary point of view, the chronology of innovations before the convergence of Information and Communication technologies. We can observe the tendency of technology Research & Development studies in different nations with this chronology.

2.4.4 Shifting from Discipline to Control Society

Discipline society was the term used by Foucault (1977) while he was working on *Discipline and Punishment*. Today the discipline society turns into control society, with support of new technologies monitoring capacities. James R. Beniger's (1986) arguments in his book *The Control Revolution* will form the basis of the arguments that follow. Our readings will then expand beyond the

[10] http://absoluteone.ljudmila.org
[11] www.ctheory.com/article/a013.html

traditional literature of the surveillance to those from sociology, political science, history, and cultural studies, and coordination and control of human activities. By the time we are finished, we will have a good overview of the literature and a robust theoretical framework for thinking about the surveillance debate. This framework will enable us to place the latest technology and policy developments within their proper context and analyze them in a historically informed way.

At the beginning we have to be critical about social change argument of him for our framing. Beniger (1986) claims that technological innovation is a consequence and not a cause of social change. There is a reciprocal relationship between technology and society in sake of change, because each affects change within one another. Either social determinism or technological determinism cannot explain the change by its own ceteris paribus.

In Control Revolution Beniger (1986) argues that bureaucracy remained the single most important 'technology of the control revolution, as Weber claimed it was the most control technology of the industrial civilization. But Beniger (1986) enlarged his control revolution theory to ICT. After Second World War general control shifted to technological control slowly. In addition to that, Beniger (1986) argues that technological revolution was also a part of control revolution.

Further Beniger (1986) claims that computer might generate a new 'intellectual technology', in which the operations can be categorized, as technology is a natural extension of the control revolution already in progress. The computer control revolution can be described as a series of basic information/communication technologies that emerged in the span of a single lifetime. The historical background of Beniger's control revolution theorization begins with the face-to-face relations before the industrial revolution, in sake of

controlling at governmental and market production actions. At industrial revolution period state and bureaucracies adopted centralization. Moreover rail and telegraph infrastructures completed the control.

Today the percentage and quality of control is directly depends on capabilities of ICT infrastructure. Therefore, Beniger (1986) says control revolution is an extension of industrial revolution with the focus on processing and controlling of information. Here we add to this point of view that the system's control effectiveness depends on the capability of gathering more and more information about every detail of ordinary people. As people turns into binary digits and barcoded controlling of the crowd becomes cheaper and easier.

The economy enlargement consisted upon these technologies of control and monitoring especially at USA and UK is really a great percentage, which we cannot pretend as if we do not recognize. So warfare at cyberspace, and market of ICT can be easily interpreted as devilish. The power of control revolution is obvious at security sector of nations. At the origin of most technologies we use today, military research and development activities exists.

Inevitable steps of control are information recording, processing and reciprocal communication channels. Information processing is a result of the comparison on future possibilities and records of current situations. The capacity to sustain control is directly related with the evolvement of 'information' technologies (Beniger, 1986).

Computers have already profoundly changed activities performed in many of society's institutions (business, banking, education, libraries). They will have

even greater effects on institutions in the future. They have also raised or caused new ethical issues, and these will need to be addressed in the interests of social stability. In addition, developments in computing have affected or given rise to other new products and methods in a variety of fields, further demonstrating the interdependence of ideas, society, and technology.

There are microprocessors in stereos, televisions, automobiles, toys and games. Entertainment and telecommunications industries are heavily dependent on new electronic technologies. Computers themselves are directly attached to research instruments that gather and interpret data in basic physics, chemistry, and biology experiments. The resulting changes and advances in scientific research have also caused profound effects on society and its institutions. They have resulted in new social and ethical questions being raised. These include issues relating to software copyright, data integrity, genetic engineering, artificial intelligence, and displacement of human workers by robots, how to live in and manage an information-based society, and how to repair damage wrought in the industrial age, such as total surveillance paranoia.

To control the citizens state needs huge detailed information of every individual, to control the consumption and benefits firms need huge detailed information about the consumers. This brought about the commodification of data that we are going to provide as a subtitle later on. To sum up, Beniger's exemplifies the principle of reciprocal control in information processing. The control revolution thesis documents the co-evolution of US rail and telegraph networks. These were explicitly informational' characterized. The control over production and distribution was later extended to consumption context, and the tool of it extended to ICT.

2.4.5 Privacy versus Secrecy

Privacy as freedom to be left alone has been distinguished from privacy as freedom from the intrusions of formal institutions and authorities. Today the meaning of the secrecy changed upon the acceptance of privacy. Intrusion to our private sphere, especially our daily life without our compromise causes one of the most popular discussions. There are different types of surveillance as we categorized somewhere above, but the main focus of this work is indirect, invisible, maybe the oldest type of surveillance. All things are naked. If you are a good citizen, employee, student etc... You have nothing to be afraid of (Lyon, 2001).

The common accepted definition of privacy is "the right to be left alone" which cannot be said equally applied. Dataveillance is firstly defined by Clarke (1988) as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" Dataveillance is initially documentary its directly related about recording of data. It's mainly about sorting and filing data about individual's record kept under the power holders who seek data in ever process of our daily lives. The more we became technology dependent in practice of life the more easy we are recorded and traced back. An unintended comprimise between the power holders and subordinated exist at data recordings. Furthermore, although with data surveillance one's transactions can be followed and information on oneself can be exchanged or scrutinized at any time, this surveillance remains indirect different from video surveillance (CCTV).

Recently technologies that affect privacy have exploded in number, complexity and power. Clarke (1988) intensified his works on dataveillance and

classified PITs and PETs PITs as a term *describes the many technologies that intrude into privacy. Among the host of examples are data-trail generation through the denial of anonymity, data-trail intensification (e.g. identified phones, stored-value cards, and intelligent transportation systems), data warehousing and data mining, stored biometrics, and imposed biometrics. PETs* are the tools which standards and protocols that set out to reverse the trend, by directly assisting in the protection of the privacy interest.

CHAPTER 3

THE TECHNO–HISTORICAL BACKGROUND OF THE SURVEILLANCE SOCIETY

To map the surveillance technologies, listing a chronology like below will help us to make an assumption, the relationship between R&D expenditures in particular countries especially USA and UK for espionage originated technologies supported by state and common sense of the social entities. The paranoia is greater about the rebels against the system at developed countries. The surveillance technologies innovations are originated from that fear. To control the masses developed equipment is necessary. Thus we can say these technological innovations flourished easily and developed in a short while in these prosperous countries and spread out the world.

Table 2:

Chronology of Technological Innovations up to Surveillance Technologies

Invention	*Year*	*Country*
Electric telegraph	1837	UK
Facsimile	1843	UK
Trans-Atlantic telegraph cable	1866	USA
Typewriter	1870	Denmark
Telephone	1877	USA
Half-tone printing process	1880	USA
Punched card	1884	USA

Cylindrical record player	1888	USA
Mechanical record player	1889	Germany
Radio	1896	Italy/UK
Vacuum tube (valve)	1913	USA
AM radio	1920	USA
Dynamic loudspeaker	1924	USA
Electric record player	1925	USA
Television	1925	UK
Magnetic tape recording	1935	Germany
FM radio	1936	Germany
Photo-typesetting	1946	USA
Transistor	1947	USA
Long-playing record	1948	USA
Xerography	1950	USA
Electronic computer	1951	USA
Color television	1953	USA
Trans-Atlantic telephone cable	1956	USA
Integrated circuit	1961	USA
Communication satellite	1962	USA, USSR
Packet switching	1964	USA
Video cassette recorder	1970	Netherlands
Fiber optic cable	1970	USA
Microprocessor	1971	USA
Personal computer	1976	USA
Trans-Atlantic fibre optic cable	1988	USA

Source: The information society by Ewan Sutherland[12]

This chronology shows the huge amount of investment made in the USA for research and development (R&D) on technology. Most of the gadgets we use

[12] http://www.lamp.ac.uk/ewan, http://sutherla.tripod.com/infsoc/inf_rev/

today are a result of this R&D. Since the US is the super power of the world, it consequently has deep impacts on today's technological developments. So we have to thank the US for both our liberalization and slavery. Especially the innovations at ICT have to be paid attention. Because New World Order myth is being established through these technologies improvements.

Technology is one of the main transforming actors of the society and its economic, political, cultural substructures. When we talk about science in general it also included technology, in meaning. The dominant role of science over technology changed vice versa. Brave or not it is a new world, in which science lost its dominant role and became subservient of technology. This new world is being established on information production, storage, exchange and analyses For that reason, the role of new information and communication technologies is vital in understanding of surveillance society debate.

Although there are conflicts in discourse, the system uses the most appropriate one and maintains its existence by different substructures reorganization, with reproduction of a relevant socio-political discourse to legitimize itself. This discourse maintains the strength of mystification of future and technological innovations effects, but also for critical textual readers the possibility of rising monitoring roles of the power agents and surveillance society debates.

The paradox of electronic surveillance is used but understood little. To clarify what is being discussed in surveillance society debate, we have to analyze the discourse. One of the signifier of our age is technology, but we do not mean it is the only source of determiner to understand surveillance society. Social dynamics have more than one face, we have to be critical and check every

qualifications of the change. We can question the technological structure of surveillance society by dividing it into parts. Here we can point out the difference between analog and digital technologies. Then we can mention convergence of information and communication technologies and their relation with the surveillance society fact. Moreover, a chronology has been included to frame developments of surveillance technologies up to now. Then, we can place Internet as a medium to understand surveillance society that we left footprints behind, in its pathways. Finally, we can briefly talk about intelligence agencies projects used for tracking data, by digital surveillance technologies.

3.1 From Analog Technologies to Digital Technologies

The first computers were using punch cards for recording the data, the machine was not practical, and the size of it was not manageable and also the speed of it was so low. The 'mini-computer' architecture emerged during the 1960s and 1970s, they were based on a different component technology, then they are matured into the 'mid-range' machines of the 1980s and 1990s. In 1980s there had been an improvement in digital technologies that aid different processes easier and faster.[13]

Digital compression techniques and the development of the Internet and broadband cable networks will provide the infrastructure for people and organizations to simply plug in a wide web of opportunities, online activities.

[13] http://www.isoc.org/zakon/Internet/History/HIT.html

We can make a citation for showing this digitilization's importance, from the author of Being Digital Negroponte, he insists that the nature of computers as digital storage devices will determine how they are used in the future. (Negroponte, 1995).

3.2 From ARPAnet to Internet

In 1969, operations began on the ARPANET, which can be seemed as big brother of the Internet. The Poorman's ARPANET, a network that was originally designed to survive at a nuclear attack, evolved into a citizens thinking pool, an intellectual marketplace, an interactive multi-access computer community today.

Network born at the cold war period from the fear of cold war paranoia. US government produced ARPANET as a response to Soviet Union's launch of Sputnik in 1957. ARPANET protected the flow of information between military installations by creating a network of geographically separated computers that could exchange information via a newly developed protocol called NCP (Network Control Protocol). Communication was an inevitable necessity for the possibility of a nuclear attack in cold war era.

The network did not depend on a particular machine, so if there was an error in one part of the network, the communication was still possible between other parts. There were two problems faced with when a web of computers tried to be developed as a network of communication. Firstly, creation of substructure consisted of switching nodes and telephone circuits, with its reliability, capacity, delay character and cost which serves for the resource sharing. Secondly, building of protocols within the operating system of each computer in the network, for

allowing sub-networks to share resources whenever necessary (Hauben 1997)[14]. The problems solved by scientist in time caused by technique obstacles. One and only centralization would disable the new system of communication; as a result of the decentralization, there were no obvious central command to be attacked. Surviving points could be reestablished, power of the network comes from its nature of being a web of dispersed control points.

There is an opposition to ARPAnet's origin proclaimed by Charles M.Herzfeld, the former director of ARPA. He claimed that ARPAnet was not created as a result of a military need, stating, "It came out of our frustration that there were only a limited number of large, powerful research computers in the country and that many research investigators who should have access were geographically separated from them." ARPA stands for the Advanced Research Projects Agency, a branch of the military that developed top-secret systems and weapons during the Cold War.

There were 10 computers connected in the original ARPAnet. They were located in the respective computer research labs of UCLA, Stanford, UC Santa Barbara, and the University of Utah. As the network expanded, different models of computers were connected, creating compatibility problems. The solution rested in a better set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol) designed in 1982.[15]

To send a message on the network, a computer breaks its data into IP (Internet Protocol) packets, like individually addressed digital envelops. TCP (Transmission Control Protocol) makes sure the packets are delivered from client

[14] http://www.columbia.edu/~rh120/ch106.x08
[15] http://inventors.about.com/library/weekly/aa091598.html

to server and reassembled in the right order. Under ARPAnet several major innovations occurred: e-mail, the ability to send simple messages to another person across the network (1971); telnet, a remote connection service for controlling a computer (1972); and file transfer protocol (FTP), which allows information to be sent from one computer to another in bulk (1973).[16]

As non-military uses for the network increased, more and more people had access, and it was no longer safe for military purposes. As a result, MILnet, a military only network, was started in 1983. Internet Protocol software was soon being placed on every type of computer, and universities and research groups also began using in-house networks known as Local Are Networks or LAN's. These in house networks then started using Internet Protocol software so one LAN could connect with other LAN's.

In 1986, one LAN branched out to form a new competing network, called NSFnet (National Science Foundation Network). NSFnet first linked together the five national supercomputer centers, then every major university, and it started to replace the slower ARPAnet that was finally quitted at 1990. NSFnet formed the backbone of what we call the Internet today. Most of the time spent in the Internet nowadays is mediated through the World Wide Web (WWW) experience produced by current browsers. However this has not always been the case, if we consider the Internet as a group of different innovations developed for different purposes, we can identify the different array of services that it offers. Ranging from electronic email, user group discussions (news groups), searching services, information retrieval, file transfer and some other "playful" activities like games or muds that have been present since the early days of computer process sharing experiments. The Internet has become a familiar "place" (cyberspace) for millions of people that every day login to exchange messages, have a chat, search for

[16] http://www.zakon.org/robert/internet/timeline

information or sell a book to mention only but a few of the activities that take place under this platform (Lynch,1993).

To trace its origins involves realizing the myriad of circumstances, people, institutions, technologies and relationships that have make it possible. This could also help to clarify some of the basic concepts and design ideas behind its current shape, and the implications of its development for society in general.[17]

The Internet in its very basic conception can be considered as a group of innovations that make it possible the communication and transmission of "data" between computers at different locations. It has born out of the idea of distribution of resources and sharing of information over computers. Should it be understood as a collection of tools, people and resources and not only as fuzzy whole that creates a virtual space. We can take the categorization of Mc Garty and Haywood for the evolution of new communication technologies (Mc Garty and Haywood 1995, p.236):

> 1. The Simple Internet (1968-1974): Arpanet was developed for the Advanced Research Projects Agency (ARPA), a part of the US Department of Defense. Arpa was the main body, which funded academic computer scientists. Arpa's funding proved the way for these scientists to create the ARPANET. The concept intended to link computer scientists and other research institutions to one of the variety of host machines at large remote computer facilities. Thereby the distant computers would have efficient access to machines available at the home institutions. The first host connected to the Arpanet was on September 2, 1969 at UCLA and it began passing bites as SRI, UCSB, and UTAH. Only the academic computer science department of Defense funding had possibility of access to Arpanet. There was no concept of user-to-user communication in the first stage. Arpanet pioneered the networking technology that serves as the foundation of today's global Internet.

[17] http://www.let.leidenuniv.nl/history/ivh/chap3.htm

2. The Internet Goes Global (1973-1981): In 1974, TCP (Transmission Control Protocol) envelopes were developed. The transmission protocol suite adopted TCP/IP for Arpanet. Originally aimed at remote login and FTP (File Transfer Protocol) the afterthought, e-mail covered 95% of total network traffic. E-mail users had access not only to remote host computers but also to many other individual users; people from elsewhere could log into them as guests. This approach influence the naming of network constituents, connected computers with users were called hosts.

The growth of the Internet led to creation of Domain Name System (DNS). It was an easier method of addressing the nodes/ servers. By using a final node after dot like as (.mil) for military bases, commercial sites (.com), government agencies (.gov), universities and research institutions (.edu), specialized organizations as (.org), and networking corporations (.net) - would be the local computer connected to net through labeling by their IP addresses. Host names were mapped to network addresses by a file on each host, and then they are updated from a master copy. This allowed Internet to become a distributed conversational medium and opportunity to create communities of commonalities. This was a considerable change in the paradigm.

3. Military and Non-Military Split (1982-1986): In this period non-military and authorized access had been realized. User scores from hacking had been observed. E- mail had been available on some sharing system since 70's but it had not previously been used on a network. Thus the great success of Internet is not technological but in human impact. E-mail may not be striking advance but it is a completely new way of communication. It quickly became the killer application, wildly popular. The development of Arpanet viewed the computer as a communication medium rather than only as a computational device.

4. The Mitotic period (1986-1992): A tool called gopher is created, and the accessibility of the net enhanced by it in 1991 by the University of Minnesota. Then cell division of the network occurred. Local and regional networks were adapted. The number of hosts grew explosively while end user access spread. On the other side, the user identity was still with the host. The major traffic was still e-mail. Access became available on

college campuses and people began using it as a part of their intellectual activity.

Internet sponsored in the 1980's by the national science foundation (NSF) as an electronic communication laboratory used by geographically dispersed researchers. Thousands of researchers and scholars in private industries connected to the Internet. The main assumption was that the system could enhance the effectiveness of research communities. So that each community was connected to others via private e-mail, public real time chat worldwide public conversations such as Usenet.

5. New User Access Era (1993-1995): In 1994, WWW (World Wide Web) and mosaic took the net. Hypertext links in documents indicated other relevant documents and it allowed easier use by a mouse pointer to select and download text, graphics and audio/video data. Roy Tomilson wrote the original e-mail program. People used it more for personal communication. So this redefinition continued the WWW. The user community was expanding from computer literates to infrequent user community.

6. The Distributed Open Network (1996-?): The network moved into a gigabyte per second backbone allowing for the first time real time access to such applications as multimedia processing. The Internet backbone was effectively being privatized and the responsibility for its maintenance and developments would result with commercial service providers, the ISP's. As a consequence widespread use of the Internet, end users access cost decreased. (McGarty, Haywood, 1995)

Technological advance lowered the cost of processing of information so that gathering storing and tracing the data became increasingly feasible. Each of us using Internet facilities with our free will but at the same time we are unwillingly participating in this surveillance action of data collecting and tracking. We buy the spy with our free will, but at the same time the invasion of privacy works without our will. Efforts of spreading new technologies and

Internet in the sake of liberating effects need to be question then. The table below shows how much individuals use it and what a huge control effect the power holder gains by Internet's spread and diffusion into mechanisms of society starting with personal usage. The table below shows the statistics about the common use of Internet:

Table 3 Distribution of Internet Users (millions)

	December 2000	May 2002
USA/Canada	177.78 (42.5%)	182.67 (31.4%)
Europe	133.97 (32.0%)	185.83 (32.0%)
Asia/Pacific	104.88 (25.1%)	167.86 (28.9%)
Latin America	16.45 (3.9%)	32.99 (5.7%)
Africa	3.11 (0.7%)	6.31 (1.1%)
Middle East	2.40 (0.6%)	5.12 (0.9%)
TOTAL	418.59	580.78

Source: History of Internet [18]

We can claim that Internet has a power in its existence more than a technological development; it is an ethical and political concept of our century. The nature of the Internet is rooted in wide-area distribution effective for constant surveillance and rapid strategic positioning of divide-and conquer strategies through distributed communications. The wide acceptance and use of the Internet turn it into a magic surveillance tool for state and online corporations. At the same time it distributes our texts for communication it distributes them for surveillance too. However, it has linguistic and cultural barriers and cannot point a pure global

[18] http://www.let.leidenuniv.nl/history/ivh/chap5.htm

market place. ‘What are the social relations of technology through which the Internet will be mediated?’ is a question as yet not replied (Dillion, 1997). [19]

To sum, Internet was as a result of the militaristic innovation, but inevitably diffused into our daily routine. We are already used to pervasive tracking of our daily routine online. Web sites immediately identify visitors based on tiny files called "cookies" placed in their hard drives. It is these trackers that allow Amazon.com to greet you by name and make suggestions of books you might like based on your past buying behavior. So powerful groups in society will study those new information technologies as heightening capabilities for surveillance and control. But Internet still has two faces it can be either the tool of individual’s or state and private firms’. This gives Internet a chaotic role as a free space for acting of different powers that is called as warfare in information age.

3.3 INTELLIGENCE AGENCIES & CROWD CONTROL PROJECTS

Global surveillance systems are not officially accepted, but by being revealed some of the internal authorities, is one of the most discussed subjects of the last decades. Echelon is one of the most famous of these surveillance projects of surveillance of the world. The difference of the echelon it is used for watching filtering and recording ordinary people without purpose, randomly selected words are being captured by this system. For example if you use bomb, Allah, and Pentagon in the sentences on the same phone call the system records this conversation. The report on written by Wright for the European Parliament shows the detail of the established surveillance system in Europe. The USA was the leader UKUSA agreement has signed by five countries USA, UK, Canada, Australia and New Zealand for the establishment of this project. Before the reveal

[19] http://mediafilter.org/caq/internic

of existence of this global surveillance system, it was the best kept secret of the world. The most frightening point is that the report claims that there is a political shift in targeting instead of investigating crime law enforcement agencies are now monitoring and tarcking for the social classes and races in the red lined areas before the crime is committed. This means a shift in one of the main acceptence of law, before until there is no evidence one has been accepted as innocence; but now until reverse is confirmed one is accepted as guilty.[20]

3.3.1 Echelon and Enfopol

Echelon is a global surveillance system gathering information all over the world. The first step in the Echelon project set by the UK-USA (United Kingdom-United States of America) agreement (1947) by which the security agencies of England, Canada, New Zealand and Australia have joined NSA (National Security Agency) of USA. Since there is no legal declaration about Echelon or even its existence, the information about the system is neither detailed nor coherent.

The first formal information was revealed by the author of the European Parliament's 1999 'Interception Capabilities 2000' report, Duncan Campbell, who defined Echelon as one of the worldwide surveillance systems that aims to "intercept messages from the Internet, from undersea cables, from radio transmissions, from secret equipment installed inside embassies, or use orbiting satellites to monitor signals anywhere on the earth's surface" [21].

[20] http://www.statewatch.org/eufbi/eufbi04/htm
[21] http://www.heise.de/tp/english/inhalt/te/6929/1.html

Several credible reports suggest that this global electronic communications surveillance system presents an extreme threat to the privacy of people all over the world. According to these reports, ECHELON attempts to capture astounding volumes of satellite, microwave, and cellular and fiber-optic traffic. The big deal about Echelon is that it tries to collect huge amounts of almost random data and sort out the interesting stuff using keywords. This is quite different to most surveillance operations, which are specifically targeted and designed for usually national military purposes.

These vast quantities of voice and data communications are then processed through sophisticated filtering technologies. This massive surveillance system apparently operates with little oversight. Moreover, the agencies that purportedly run ECHELON have provided few details as to the legal guidelines for the project. Because of this, there is no way of knowing if ECHELON is being used illegally to spy on private citizens.

While the NSA will neither confirm nor deny the existence of the ECHELON system, a report commissioned by the European Parliament last years confirmed that every communication in Europe has been subject to surveillance for years and the system can decode any clever encryptions. More alarmingly, European business intelligence has been known to leak from the NSA to American businesses, providing American businesses with illicit information on mergers, take-over and bids. Since there are so few details available, Echelon can inspire paranoia. But you can be sure it exists, just not sure how big it is.[22]

Recent resistance and legal protests against to Echelon by EU is more related with the economic lose of themselves. USA is using economic

[22] http://www.thirdworldtraveler.com/New_World_Order/Eavesdropping_World.html

informations in its benefit and strengthened the crucial trading positions between the other nations'. To exemplify reported in The Sunday Times (11 may 1998) Airbus Industrie lost a contract worth 1 billion dolar to Boeing and Mc Donnel Douglas the reason was he USA interception of communication.[23]

Although the cold war said to be ended, still mechanisms of hegemony are on duty. The balances of world depend on espionage. European Parliament rejects Echelon but now establish their own filtering system in the name of secrecy, called as Enfopol. In February 1997, Statewatch reported through this secret network "EU countries it says, should agree on "international interception standards set at a level that would ensure encoding or scrambled words can be broken down by government agencies."[24]

3.3.2 Carnivore

Carnivore the best-known and most controversial tool used by the federal government is one of many Internet traffic-capturing tools designed by the FBI. Carnivore been mentioned in a package called "DragonWare Suite". The official release on this suite states:

- Carnivore – A windows based program that captures packet information.
- Packateer – No official information.
- Coolminer – No official information.

[23] http://www.europarl.eu.int/stoa/publi/166499/execsm_en.htm
[24] http://www.europarl.eu.int/stoa/publi/166499/execsm_en.htm

It is theorized that the Packateer and Coolminer programs are filters designed to pick out specific passages of e-mail and/or packet information. One of the main problems for creating awareness about surveillance supervision characteristic is that inability of taking official true information. In our conclusion we are going to specify the reasons behind these and make some suggestions.[25]

Carnivore, based on the information released by the FBI, is a sniffer, which is placed on the back end of an ISP to watch the movements of a specific user. There are similar systems administration tools available for public use on the Internet. Carnivore captures the targeted packet data traveling over the suspects Internet service provider (ISP) network. The data is then filtered to check for specific patterns or information. Any information not intended for the eyes of the law enforcement officials as specified in the court order, is discarded while a copy of the filtered information is saved onto hard drive for possible future use in a case against the suspect.[26]

- The Carnivore system is a personal computer running Windows and is equipped with a network card and Jazz drive for removable disk media.

- Since Carnivore must be physically connected to the network in order to monitor it, the computer is installed at an Internet Service Provider, a university, company, or other organization that provides Internet access for the person to be monitored.

[25] http://www.FBI.gov/hq/lab/carnivore/carnivore.htm
[26] http://email.about.com/library/weekly/aa102901a.htm

- Once installed, Carnivore uses a packet "sniffer" to collect all data that passes through the network. At an ISP, that includes all emails sent and received by its users, the content of all the Web sites they visit, or all messages sent through an Instant Messaging application, and all other network activity, too.

- The aggregated data is sent through an aggressive filter that discards all information that is not to or from the person subject to a wiretap order.

- Additionally, Carnivore can distinguish between communication that may be lawfully intercepted (emails, for example) and communication that must not be intercepted. All data passing the filter is written to the removable disk. A FBI Special Agent coming to the site and put in a sealed box collects disks. Additionally, the fundamental problem with this kind of surveillance technology still applies:

- While the physical installation of Carnivore devices can be monitored, it is difficult if not impossible to control which data is actually collected. Carnivore is capable of harvesting all of an ISP's traffic if its filters are put out of place or reconfigured. Nobody outside the FBI has the source code to the Carnivore software or knows the actual configuration of Carnivore's filters.

3.3.3 Magic Lantern

One other possible aspect of the "Cyber Knight" Internet dragnet is the "Magic Lantern" program. Bob Sullivan of MSNBC first wrote about the Magic Lantern project when the Electronic Privacy Information Center (EPIC) requested information on the subject under the Freedom of Information Act. Sullivan describes the Magic Lantern project as a key-logging program, which captures the crypto key from a suspect's computer. Crypto keys are the cornerstone of such programs as Pretty Good Privacy (PGP), and are used to encrypt electronic mail. Only the intended reader holding the corresponding key can unlock/unencrypt the email.

Magic Lantern is more a Trojan horse than anything else. Some have called it a virus, but, as you know, viruses are destructive in one-way or another, hence the name. It is not related to worms because worms propagate from one computer to another usually through e-mail. Magic Lantern would infiltrate a suspect's computer as an e-mail attachment or possibly trick the user into downloading the program from a website. It's theorized that the program will sit in the background, on any Windows system, and wait until the request for the encryption key is made. The request activates the program, which captures the encryption key. Once the FBI or investigating group has the encryption key of the suspect, they would then be able to read the encrypted e-mail. [27]

[27] http://www.magiclantenshows.com/

CHAPTER 4

SURVEILLANCE SOCIETY

The discursive background has to be understood to clarify the interactions in the system. Foucault's work was one of the best know on discursive ideological analysis of this disciplinary society through the work of Bentham. Common used concepts such as postmodern, global, revolution can be given as examples to these background noises in our age.

4.1 Surveillance Society Debate

Surveillance, monitoring, tracking, supervision, observation, spying, snooping, espionage, prying, sneaking, voyeurism, etc. When we take into account these words used to define as an adjective of contemporary society we can figure out inspection of power holders and the gaze, the visual image or being seem, being watched exist at the center of the discourse in many realms of today. There are some intuitive sociological studies done on the broader subject of surveillance, a subject area that has emerged from the sub-disciplines of the sociology of technology, deviance, social control, mass communications, bureaucracy and complex organizations (Rule 1973; Marx 1988; Dandeker 1990; Gandy 1993; Lyon 1994; Bogard 1996). Surveillance has been broadly defined as "any form of systematic attention to whether rules are obeyed, to who obeys and who does not, and to how those who deviate can be located and sanctioned" (Rule,

1973:40). According to David Lyon the societies that are dependent on communication and information technologies for administrative and control processes are surveillance societies. The effects of this are felt in ordinary everyday life, which is closely monitored as never before in history. Until modern times the scale was generally small and the watching unsystematic. Today, routine, ordinary surveillance, usually mounted by agencies and organizations that are geographically remote from us is embedded in every aspect of life (Lyon, 2001).

Surveillance society is relatively a new research subject because of that usually a study written about it depends on the same cross-references. There is more material on video surveillance then dataveillance, maybe the cause for that is invisible characteristic of dataveillance. Maybe its more embedded in structures of society and its history can be traced back to ancient times to the pictures on the cave walls. Surveillance takes two forms as described by Giddens (1985):

Firstly, direct supervision of the work of subordinates by superiors. Secondly, indirect surveillance, which is, consisted of records, kept files, case histories. As we all mentioned before our focus is this data recording and tracing. Max Weber saw the importance of written records and wrote about it but could not figure out how they regulate human behavior. Records used to monitor employee by owners of the production. Performance controlled in organizations by tracking the records. In modern organizations surveillance is important because of their strong reliance on disciplinary characteristics. The industrial revolution with establishment of factories forced people to work in limited hours under control of the owners of the capital. The people were not used to it in general traditional ways they had worked, as they needed. The architecture was planned for constant supervision.

Foucault set out his works on discipline and surveillance on Bentham's panopticon, and states *surveillance* as an ideological control tool by itself. He lays great emphasis on how visibility or lack of it influences and expresses patterns of authority in the architectural settings of modern organization. How far what subordinates do is visible to those of higher grades affects whether they can easily be subject to what calls surveillance. Surveillance refers to supervision of activities in organizations. In modern organizations everyone is subject to surveillance. Relatively higher positions are less scrutinized than lower positions (Thompson, 1967 cited in Giddens; 301). In addition to that, we can make observations for visibility in daily life at different organizations separation of the working places and prison cells is designed for supervision and coercion. In Foucault's words they efficiently distribute bodies around the organization. Timetables were a tool for discipline founded in organizations that helped to control movements of the workers in a schedule. Observers could recognize the lacks in work by controlling the timetable. A timetable makes possible the intensive use of space and time. Every break down of efficiency can be managed by the strict measurements of time schedules. A timetable is a kind of control mechanism of free slaves of modern times. In theory workers are free to sell labor and time of them different from the slaves. The paradox exist here, do they have an alternative in practice?

Today the use of time and space independency as a discourse of new technologies legitimization is not coincidental. As we mentioned before time and space independent individuals dreams to be free of its chains so that market fakes them as if they are being liberalized from time and space limits by developments at ICT.

Foucault and Goffman focused on the organizations in which individuals are physically separated from outside world for long time periods. In those kinds

of organizations individuals are hidden away the external environment factors, so they are usually described as carceral organizations. Goffman defines prisons; asylums and carceral systems differentiated from other organization types because of their “totally closed” nature (Goffman 1961). Moreover, Foucault tried to show that the study of carceral organizations can illuminate the other organizations running.

Without doubt the ruling classes have merging state power surveillance on their agenda. Developing techniques of social control had been very important in history. While enhancing efficiency and productivity, surveillance also focuses on a functioning bureaucracy to maintain power and control. In addition, functioning surveillance systems are even more important in times of economic crisis and during times of war. It is the rise of new technologies that has enhanced the opportunities for the main aims of surveillance such as control and discipline. Technology does both, enabling globalization processes and widening the opportunities for social control. With the ongoing fragmentation of advanced post industrialized societies caused by the “neoliberal project” a new trend emerges, from ‘simple’ control and discipline of people to identifying and classifying them, the social sorting of people. Profiles of individuals have been created from gathered data about them. Controlling crowd is dependent on gathering more knowledge.

In the years separating the original design and the complete, working version of the difference engine computers developed beyond 'number-crunching' into communications, information management, entertainment, education and almost every other field of (Western) human attempt. Because of this there has been much of what Paul Virilio, in his book 'The Vision Machine', calls 'frantic interpretosis'. Under the influence of this 'frantic interpretosis' the computer has been credited with a gradual destruction of social life or, conversely, offering the

possibility of a techno-utopia. If some commentators are to be believed there will soon be a networked 'perfect' democracy where every individual will have access to all information at all times and be able to communicate with any other user by e-mail or video conferencing. As Hiltz and Turoff (1978) propose, 'We will become the Network Nation, exchanging vast amounts of information and social-emotional communications with colleagues, friends and "strangers" who share similar interests ... we become a "global village" ... An individual will, literally, be able to work shop, or be educated by or with persons anywhere in the nation or in the world.'

Critical theory, particularly Derrida and Lacan, had already reconceptualised (Sarup, 1993) and undermined traditional ideas about the relationship between language and the subject and also the apparent stability of the concepts language and the subject themselves. The subject, as it is drawn from the great traditions of Western thought functions as a centre point from where it can survey the world and its objects. According to this tradition, also, language functions as a direct translation of reality. However, I will attempt to show that this reconceptualisation coincides with a disruption and a destabilising from another non-philosophical direction. In many ways the new electronic, networked environment of the internet, hypertext and the world wide web embody these developments in critical theory and put them into practice, they also suggest new avenues of investigation and shed new light on this relationship between the subject and language.

Different scholars conceptualize the age we are facing with in various ways, but our main focus will be is at the subject of improvements in new rising technologies and their sociopolitical and socio cultural ends in the sake of surveillance context. Information age is a phenomenon used commonly in social science debates. Being a buzzword makes the conceptualization more difficult and

blurred. The world is in a transformation period. However, we would not accept a revolution of information without questioning. Why it is claimed to be a revolutionary change? Is the cyberspace a real freedom space for all, or is this a manipulated myth for free market. Although, we cannot ignore benefits of internet, we have to be aware of its coding opportunities in everyday life for the owners of power, which can also mean an death of privacy, without our will.

The tremendous explosion in surveillance-enabling technologies, including databases, computers, cameras, sensors, wireless networks, microchips, GPS, and biometrics. The nightmare of Orwell's vision about "Big Brother" is technologically possible in these days.

Surveillance video cameras are rapidly spreading throughout the public arena, with new cameras being placed not only in some of our most sacred public spaces, but on ordinary public streets all over America, UK and the world. Moreover, video surveillance may be on the verge of an even greater revolution due to advances in technology like Face Recognition Technology and new attempts to build centralized monitoring facilities.

An insidious new type of surveillance is becoming possible that is just as intrusive as video surveillance what we might call "data surveillance." As more and more of our activities leave behind "data trails," it will soon be possible to combine information from different sources to recreate an individual's activities with such detail that it becomes no different from being followed around all day by a detective with a video camera. Video surveillance is not directly related with citizenship but dataveillance is. To exist and to practice daily life one has to be involved in some of these databases especially basic birth records, or ID cards.

Computer databases are controlled by larger bureaucratic institutions and play a greater role in citizenship, employment and consumption than cameras, and therefore they influence the everyday lives of citizens, employees and consumers more than do cameras. The threat of the "panoptic sort" and other manipulations of one's data image, *digital persona*, are very serious and real (Gandy, 1993).

4.1.1 Globalization as the Supporting Sub-discourse

The development of information technologies, that are the prime focus of this thesis, and their spread to all corners of the earth, is a late 20th century phenomenon even though the scientific basis of these technological developments were laid in earlier decades. More particularly, the rise of cross-border communications in a variety of forms, such as satellite connections, computer networking, and international telephony, coincides with a period of multifaceted social transformation, which came to be called as “globalization”. Therefore, any discussion of information technologies’ impact on social relations, including the issue of surveillance, would be incomplete unless sufficient regard is given to its socio-historical background, which can be examined under the rubric of globalization.

For one thing, globalization, as a concept, is as thoroughly contested as the other concepts, which are covered in the previous chapters. Notwithstanding the statement in the previous paragraph, there is no agreement on its chronology, as well as on its definition, explanation, measurement, and normative assessment, policy implications and even on its “global-ness”. In terms of chronology, to begin with, some scholars trace the beginnings of global relations to the first few hundreds A.D., some to 1500s, to the Age of Discoveries, still others to 19th century. There are also those that consider globalization as a phenomenon of the

second half of the 20th century, and tie its rise to the advent of modern communication and transportation technologies. This discussion on chronology is closely related to another one on the novelty of developments that comprise globalization. For some students of globalization, what we face is a phenomenon completely new and unprecedented in history. On the other extreme, scholars spend considerable energy to empirically show that the cross-border mobility of goods, people and capital is not peculiar to the age of globalization (Held, 1998).

At the heart of above-mentioned discussions lie deeper disagreements on the definition of globalization and on the range of processes that comprise it. While the intricacies of this debate is beyond the scope of this thesis, it is nevertheless possible to come up with a descriptive account of globalization drawing on a number of points on which students of globalization seem to, more or less, agree. In this respect, globalization will be taken as a process that involves:

> … a stretching and deepening of social relations and institutions across space and time such that , on the one hand, day-to-day activities are increasingly influenced by events happening on the other side of the globe and, on the other, the practices and decisions of local groups or communities can have significant global reverberations (Held, 1998: 13).

Then, in what areas of social reality can be observed such geographical expansion and intensification, or the rise of "supraterritoriality" in Jan Aart Scholte's (2000) words, can be observed? The most obvious field, one that figures prominently in any discussion of globalization, is the global economy. International trade has reached unprecedented levels recently in terms of quantity, as well as in terms of the number of goods traded and the countries involved. Similarly, the current mobility of capital in the form of global financial flows is unmatched in any earlier period of history both in terms total amount as well as

rapidity. There is a growing integration of capital markets around the world as exemplified by the global repercussions of the 1997 East Asian financial crisis. In the realm of production, production of an increasing number of goods is organized globally through an international division of labor. Multinational corporations (MNCs) are the main actors in the global production process, accounting for a quarter to a third of global output. MNCs are active not only in production but in the global delivery of a growing number of services such as insurance, banking and communications.

Another area within which the impact of globalization is strongly felt is culture. Thanks to global communications and media networks, a considerable number of cultural products are consumed at a global scale. English language has dominated others in the global exchange of information and ideas. Every year, more and more people travel abroad and encounter other cultures as the cost of international traveling decreases. For some, these developments meant the dawn of a global culture, or a cultural homogenization process. For others, on the other hand, it is an indicator of increasing cultural heterogenization, as local identities reassert themselves against the unifying tendencies of globalization. And not very surprisingly, some opted for a mid-way in the form of rising hybrid cultural tastes (Scholte, 2000). Leaving aside these assertions, one thing is clear that it is no longer possible to talk about self-contained national and/or local cultural practices not influenced by global cultural forces one way or another (Held, 1998).

Environment arguably provides us with arguably the most powerful and vivid images of the process of globalization. Global warming, depletion of the ozone layer, nuclear contamination, the loss of biodiversity and many other ecological problems threaten all the humankind in the sense that their adverse effects for human populations are experienced globally.

Globalization also has implications on how human communities are governed around the world and how politics is conducted. One of the developments associated with globalization, in this respect, is the rise and proliferation of supraterritorial, as well as sub national, regimes regulating numerous fields of human activity requiring collective action from postal services to financial transactions, from disarmament to carbon emissions, from international standards to transborder aviation. (Rosenau, 1995). In fact, this issue is closely connected to one of the hottest debates in the globalization literature, namely the fate of the sovereign statehood. The rise of supraterritorial forms of governance, sponsored and supported by both governmental and non-governmental actors, along with economic and cultural globalization, is said to erode state sovereignty irreversibly. Again, at the opposite end of the debate are located those who claim that the state is here to stay with us for the foreseeable future, and even that globalization consolidated the state's prominent position in international politics.

Having delineated the general contours of the globalization debate in a rather sketchy manner, we can now ask how recent technological developments in general, and those in information technologies in particular, fit into the context of globalization. There is no easy answer to this question to say the least. Yet the issue of causation can be a good starting point.

Two general positions on the issue of what causes globalization can be identified: structural explanations and actor-oriented explanations. On the structural side, capitalism as an economic structure and rationalism as a knowledge structure can be pointed out. With regards to actor-level explanations, technological innovation and enabling regulatory frameworks are the two main causes of globalization highlighted in the literature (Scholte, 2000). Preferring one of these explanations to another is largely a methodological question, and touches

upon one of the perennial discussions in social science, namely structure-agent dichotomy. However, it is also an ideological question in the sense that individual-level explanations have a strong tendency to overlook the structural factors, and hence power relations that underlie the current shape of globalization. After all, "Theory is always *for* someone and *for* some purpose" (Italics in the original, Cox, 1996: 87).

Technological developments in the area of communications and transportation have indisputably facilitated the creation of supraterritorial social relations in the form of global flows of goods, services, capital and ideas, comprising globalization. However, an attitude, which points out technology as the main cause of globalization, falls within a particular theoretical mindset known as technological determinism as we mentioned below in *theoretical perspectives for reading new technologies and surveillance*. Individuals do not make choices in a social vacuum. Neither do they find the incentive to invent and develop new technologies free from structural constraints such as the needs of capitalism to spread across the borders for further capital accumulation and the enabling rationalist mindset. What concerns us here is that a technological determinist approach is typically prone to mystify technological development, in the sense of attaching an essential goodness, and consequently globalization.

In this respect, an unquestioning attitude towards technology and globalization are closely related. Here, one moves into the normative terrain in the globalization debate or whether we approve of the developments associated with globalization that are briefly mentioned in the previous paragraphs. To begin with, neo-liberals typically welcome the processes of globalization, and associate it with progress, human betterment and increased welfare for all humankind. Neo-liberalism, which can be seen as a late 20th century revival of classical liberal ideas, is characterized by a strong belief in markets as the best mechanism human

beings can organize their societies, and a strong dislike for state intrusion into the workings of the market. Consequently, trade liberalization, deregulation, the shrinking of the public sector and the spread of open markets all around are all welcome developments for neo-liberals. The alleged erosion of state sovereignty, due to the state's increasing inability to control the forces of globalization capitalizing on new technologies, is also something about which neo-liberals are extremely content (Gill, 1995). The globalization of trade, finance and production are seen as the key to human prosperity, and thanks to new technologies the global hold of the markets is getting stronger. Information technologies, in this respect, enabled the most efficient allocation of resources, and production facilities. They help companies to determine the consumer taste instantly and restructure their production accordingly. The advent of global consumer preferences through cultural globalization is also a great help to global companies since it opens up ever-new markets for an increasing number of products. On the political side, neo-liberals actively support the replacement of authoritarian regimes with liberal democracies, and believe that open markets are the key to strong democratic institutions.

All these assertions can be challenged, and in fact are extensively challenged in the literature, from the perspective of human equity, democracy and freedom. In line with the central argument of this thesis, the last group of critiques, on the technology's relationship to human freedom concerns us the most here even though it is nearly impossible both practically and theoretically to divorce human freedom from questions of equity and democracy. More particularly, the purpose of this thesis is to see the power and information relationship from the perspective of surveillance, especially supervision that society subject to by state or corporations.

4.1.2 Focus on Panopticon: Bentham, Orwell, Foucault

In 1791, Jeremy Bentham proposed a new era in penal reform with the publication of his book, Panopticon or The Inspection House. He envisioned novel prison architecture based on a simple idea: implied surveillance. A central tower was placed at the hub of a circular building, the individual prison cells fanning out from this tower. The key to Bentham's design was the tower's visual supremacy. All inmates could see the tower, the tower could see into every cell. But inmates never knew neither was anyone in the tower and nor were they watching. Bentham suggested that this ever-present surveillance, whether actual or implied, would stop the inmates of his Panopticon from behaving in an inappropriate manner. The inmate becomes the controller of himself, because of the panoptic fear of watchman.

George Orwell, in his famously dystopian novel 1984, generalized Bentham's ideas from a single building to social control on a grand scale. His characters lived in a society under constant surveillance, where every word they utter, every gesture, every thought could become evidence of their own guilt. Furthermore, as in the Panopticon, this surveillance is never relegated to the background. The inhabitants of 1984 are constantly reminded of their subjugation, the main idea was similar in both, fear and possibility of a *Big Brother's* gaze.

> Though the sun was shining and the sky a harsh blue, there seemed to be no colour in anything, except the posters that were plastered everywhere. The black-moustachio'd face gazed down from every commanding corner. There was one on the house-front immediately opposite. **BIG BROTHER IS WATCHING YOU** (Orwell, 1965).

36 years later - in 1984 - Michael Radford directed the most celebrated film version of the book. To the digital generation, many of whom had never read the novel, Orwell's all-seeing, all-knowing Big Brother was represented by large computer systems. Each adult in the developed world is located, where Nineteen Eighty-Four finds its most popular parallels. In Orwell's fictional Oceania, a mass of "telescreens", complete with microphones and speakers, watched over every square inch of public and private space. These devices, centrally monitored, began their life as public information systems, and ended up policing the morals, thoughts and behaviour of all citizens. They enforced the will of the State. The relevance of Nineteen Eighty-Four to the world of the 21st century has been ferociously debated. 1984 was, largely a satirical view of the abuse of power - most notably Stalinism, and was certainly not a prophecy about the perils of technology, but today it has turned into a widely used term to define perils of technology.

It can, nevertheless, be argued that a prophet does not cease to be a prophet merely because he fails to wear the nametag. To millions of people, Big Brother presents a warning about the creation of a surveillance society through information technology. The concepts contained in Nineteen Eighty-Four have become the most powerful and enduring expressions in the privacy vocabulary. Many of Orwell's ideas have become embodied in modern surveillance societies. It is the way governments promote surveillance that most closely parallels the Orwellian State. In Nineteen Eighty-Four, the government routinely used to obverse words and images to create a false reality (its propaganda arm was called the "Ministry of Truth"). Today, the UK Department of Trade and Industry and its US counterparts consistently promote Escrow, Trusted Third Party (TTP) programs and other privacy-hostile initiatives as if they were privacy friendly technologies.[28]

[28] www.pco.org.hk/english/infocentre/ files/davies-paper.doc

Michel Foucault revitalized the panopticon as a symbol for contemporary methods of social control in the late 1970's. Calling upon his early studies of eighteenth-century medical architecture and penal reform, Foucault explored the organizing and isolating tendencies of the panopticon in a series of works. In his book Power/Knowledge, Foucault invoked the panopticon with its promise of seeing-without-being-seen as a symbol of the ultimate power of authority: "There is no need for arms, physical violence, material constraints. Just a gaze. An inspecting gaze, a gaze which each individual under its weight will end by interiorization to the point that he is his own overseer..." Foucault added, about the back lighting of the cells in the prison that was a contrary method to dungeons darkness, "Full lighting and the eye of a supervisor capture better than darkness. Visibility is a trap."

Foucault took it a step further than Bentham, however, by showing how such a concept could be applied to the late 20th century. The major effect of such panopticism, he wrote, is "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. Panopticon represent the power of the State, and helped entire generations to express their fear of intrusion by authority.

The potential to automatically match CCTV images against databases of digitized passport photos, driver license photos, and "mug shots" from existing police databases has exercised the imagination of privacy advocates and campaigners. Face recognition software, which claims to provide a "search and identify" function across entire databases of images is now commercially available.

The 1990s appear to be an exciting period for conspiracy theorists. Recent revelations about a vast web of covert national security signals intelligence operations together with evidence of endemic surveillance of the telephone system have become chat subject commonly used in some European countries. Only a couple of years ago this claims were the province of science fiction.

In 1998, members of the European Parliament (EP) were told that the US National Security Agency (NSA), in collusion with the British Government, has created the means to intercept almost every fax, email and telephone call within the European Union. Sketchy details of the NSA's spying activities in Europe have been common currency for decades, but had never been formally acknowledged. The current debate over NSA activities has erupted because of two recent European Parliament studies that confirm the existence in Britain of a network of Communications Intelligence bases operated by the NSA. These recent events have left observers contemplating two profound conclusions. First, the NSA and its partner agencies can now intercept most communications worldwide. Second, the distinction between traditional police and security agencies has been blurred.

The publication in 1997 of the first EP report, "An Appraisal of the Technologies of Political Control"[29], confirmed that the NSA had established a surveillance capacity over the entire European communications network. It also described a grid of supercomputers known as ECHELON, capable of scanning vast areas of the communications spectrum to detect keywords. Of particular interest to the Parliament was the report's assertion that the NSA was beefing up its commercial espionage activities. According to evidence presented to the Parliament, the NSA has been routinely intercepting sensitive traffic relating to

[29] http://www.europarl.eu.int/stoa/publi/166499/execsum_en.htm?redirected=1

bids, takeovers, mergers, investments and tenders for the economic benefit of the US.

Parliamentarians in Germany, Norway, Italy, Denmark, Holland and Sweden have subsequently raised concerns. Then, in September, the plenary session of the European Parliament took the unprecedented step of openly debating the activities of the NSA. In a Consensus Resolution of all major parties, the Parliament signaled its concern by calling for more openness and accountability of this once hidden activity.

In 1999, a second EP report, "Interception Capabilities 2000" set out the technical specifications of the interception system. The report describes a secret plan by US and EU authorities to create a "seamless" web of telecommunications surveillance across all national boundaries. The strategy is advised by national security agencies and by the FBI, which instigated with Brussels a top-secret planning organization called the International Law Enforcement Telecommunications Seminar (ILETS). In time two vast systems - one designed for national security and one for law enforcement - will merge, and in the process will compromise national control over surveillance activities.

In Washington, the House Permanent Select Committee on Intelligence has ordered the NSA to hand over documents relating to Echelon. The NSA has - for the activities against Robert Dean lawyer in the movie of enemy of the state were disguised as an "FBI Training Operation" - a mandate that could never be checked by an outside authority. The ability of the NSA to interface at will with private sector organisations was also featured. At one point, NSA operatives masqueraded as Washington DC police to gain access to information from a city camera network. The Agency could, likewise, access banking records, telephone

records and government agency files. The most important element of the film is probably its' focus on the absence of oversight or democratic process over such agencies. The illegal system called DIAL (Direct Intelligent Access Listening, supplied in the UK by Lorraine Electronics) DIAL allows an operator to monitor conversations in several rooms from an unlimited distance without the use of transmitters. Up to four concealed microphones are connected to the telephone line, and these can be activated and controlled by making a "coded" telephone call to the building. It is entirely powered by the telephone line and will function maintenance free for several years.

One enduring lesson of the film is its clear message that surveillance has become a design component in all information technology. Data collection is now viewed as a "value added" element of IT systems. Systems architects are required to design technology, which will capture, analyze and present personal information. Surveillance by government sits at the core of communications systems. Telecommunications companies are required by law to ensure that their equipment is "wiretap friendly". [30] As the dominant political power, the state wields the greatest ability to promulgate and institutionalize specific myths through established channels.

ACLU's (American Civil Liberties Union) president Barry Steinhardt claims that foreseeing of the Orwell is not a dystopia anymore but a real fact for the USA with 1984's the Big Brother character. After thirty years from Orwell's writings, it's all too clear that we're living in a world of visible and unverifiable power, a world where the police are pushing for the greater use of surveillance. In public places, the Report projects, we soon could be constantly monitored, due to the combined impact of recent technological advances and government initiatives. Increasing numbers of police and private security cameras mean we'll never be

[30] http://www.pco.org.hk/english/infocentre/files/davies-paper.doc

safe out in public. Meanwhile, we'll need to worry about the "data trails" we leave in places such as broker's and doctor's offices too. And even at home, our online activity could be closely monitored through further "data surveillance." "Many people still do not grasp that Big Brother surveillance is no longer the stuff of books and movies," said Barry Steinhardt, co-author of the ACLU report. "Given the capabilities of today's technology, the only thing protecting us from a full-fledged surveillance society is the legal and political institutions we have inherited as Americans. Unfortunately, the Sept. 11 attacks have led some to embrace the fallacy that weakening the Constitution will strengthen America." "Even if TIA (Total Information Awareness) never materializes in its current form," Steinhardt said, "what this report shows is that the underlying trends are much bigger than any one program or any one controversial figure like John Poindexter." An overview of the ACLU report provides information on a wide variety of surveillance issues, and their controlling role over society.

4.1.3 Categories of Surveillance Technologies

Although we focused on dataveillance there are also some other surveillance techniques. To frame the curiosity of the superpanoptic cage in which we live, we should have a look at categorization of surveillance technologies and analyze them. To have more information about them means to know the ways to resist them. The below categorization chart has been taken from the source of US Congress Office of Technology Assessment.

<u>Electronic Eavesdropping Technology</u>

- (*Audio Surveillance*)

- Radiating devices & receivers (e.g. miniature radio & ultrasonic transmitters)

- Non-radiating devices (eg wired surveillance systems including phone taps and concealed microphones)
- Tape recorders
- Laser-facilitated listening devices, rifle mikes and other "remote " equipment (incl. satellites)

Optical/Imaging Technology

- (*Visual Surveillance*)

- Photographic techniques (incl. zoom lens and infra red cameras)
- Television (e.g. closed circuit)
- Night vision devices (e.g. image intensifiers)
- Satellite based viewing (up to and including the monitoring of writings as they are written; indoors)
- Aircraft facilitated viewing

Computer and Related Technology

- (*Data Surveillance*)

- Microcomputers - decentralisation of machines and distributed processing
- Computer networks
- Software (eg. expert systems)
- Pattern recognition systems
- Voice Activated & thought activated computers (incl. "remote" equipment)

Sensor Technology

- Magnetic sensors
- Seismic sensors
- Infrared sensors
- Strain sensors
- Electromagnetic sensors (incl. brain wave sensors)

Other Devices and Technologies

- CB radios
- Vehicle location systems (incl. satellite tracking)
- Machine-readable magnetic strips
- Polygraphs
- Voice stress analyzers
- Laser interception devices
- Cellular radio
- Anti personnel weapons - sonic and phasar weapons as well as psychotronic weapons; which target the nervous system. (These have been trialed in riot control in France etc)
- Scalar wave weapons - (scalar waves emanate naturally from living organisms and the earth itself).
- Infrasound weapons - inducing various forms of illness from remote sources (Also used on dissidents in France)
- Neurophones and similar (more advanced) technologies - Satellite or ground based. These can deliver aural harassment via microwaves or lasers aimed at the target.
- Visual harassment laser systems. These deliver blurred vision, holographs and so on to disorientate the target and/or experiment; victims' reactions being monitored to study how best to "control" targets.
- Brain wave monitors/analysers (remote sensing). These newer technologies actually allow the target's thoughts to be interpreted.
- "Over the horizon" technologies - These facilitate ground-based methods of harassment.

These huge categories show that the surveillance is a great threat over all. We are unaware of the big picture of Big Brother's possibility. The great affect of the surveillance technologies are eliminated and altered with common discourse. The data is being gathered in the name of efficiency in

bureaucratic processes, personal health and DNA records are integrated into smart ID cards with chips. The CCTV is being used for security purposes to protect us from criminals. All these are common discursive stories to lower the awareness of individual about the big picture of suppression and control. To battle is impossible without definition of the enemy. Only dataveillance is in scope of our work.

4.1.4 New Data-Gathering Technologies and Dataveillance

In the near future, new technologies will continue to fill out the mosaic of information it is possible to collect on every individual; examples include cell phone location data, biometrics, computer "black boxes" in cars that "tattle" on their owners, and location-tracking computer chips (Lyon, 1994). As more and more of our activities leave behind "data trails," it will soon be possible to combine information from different sources to recreate an individual's activities with such detail that it becomes no different from being followed around all day by a inspector with a camera. Any consumption activity, which is not being tracked, has been accepted as a loss of economy. The reason behind is commodification of information about ordinary people valued as so profitable.

Firstly, *dataveillance* has been defined by Roger A. Clarke as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 1988).[31] As the number of databases that hold information on individuals grows then the subject increasingly becomes the sum of that information, or begins to be defined by that information. How we are seen and how we see ourselves will increasingly be determined by this information. Identity is central to modern popular discourse.

[31] http://www.anu.edu.au/people/Roger.Clarke/DV/NotesDVEras.html

Human identification with help of new technologies became the main subject that enabled data surveillance. As a consumer or a citizen people are separated with detailed data profiles from each other. Personal computers, personal e-mail addresses, personal banking services, etc... builds up our identities. Visual and electronic surveillance have been complemented, and are increasingly being supplanted, by surveillance of individuals and populations through the copious data trails that are generated about their activities. Mass dataveillance provides an efficient means of monitoring large numbers of people in order to generate suspicion about specific individuals and select them for closer attention. Larger numbers than ever before can be subjected to more intensive personal dataveillance, because the techniques are largely automated.

Social security cards, library cards, drivers' licenses, supermarket loyalty cards, credit cards and so on are all encoded with information about the individual and when used they pass this information on to a database so that each transaction maybe recorded. In this way a detailed picture of an individual can be built up. With the introduction, and the increasing use, of the Internet for shopping and also job application, house buying and even banking the number of these databases is increasing magnificently. The Internet user may have access to a huge database of product information but in return the user provides these 'on-line' organizations with invaluable 'client' information. It is possible to say that the user/subject may have an image of the product/object but the product/object also now has an image of the user/subject. Not only we limit the work we do at the computer, but also computer limits what we do. There is an active interaction between tool and human being (Perrolle, 1996).

This shift from absence and presence to pattern and randomness is also increasingly apparent in our lives. In an increasing number of 'everyday' situations and environments the presence of a subject is also being supplemented by a

pattern, in electronic banking a pattern in the form of a password or key number are used to access an account. DNA samples (a pattern) taken at the scene of a crime can place a defendant as can an eyewitness (a presence). The right of entry to computer systems and an increasing amount of information is determined not by any presence but the knowledge of a pattern, a code, a password etc. An illegal entry into a network by a hacker is noticeable through a coded trace rather than a physical trace of presence. Also, significantly, a pattern can represent or perform tasks for a subject on the network, web, Internet in the form of a personal/intelligent agent. These programs can respond automatically to e-mail, search out information for a subject or provide/deliver information on a particular subject.

Under these new conditions texts (verbal and visual) and bodies (textual and human) have been altered by becoming a pattern rather than a presence. Social security cards, library cards, drivers' licenses, supermarket loyalty cards, credit cards and so on, are all encoded with information which is passed to a database so that details of each transaction may be recorded. In this way a detailed picture of an individual, its movements, habits, preferences, and spending patterns can be built up. With the introduction, and the increasing use, of the Internet for shopping, job application, house buying and banking the number of these databases is increasing exponentially. The Internet user may have access to a huge database of product information but in return we can say that these products, or the organizations which promote or sell them, also have access to information about the user.

'The return channel in an interactive system will transmit back to industry much relevant information about consumer demand and consumption. This information will include the consumer's identity, the time and place of consumption and product characteristics. This data will generate an invaluable

portrait of consumer activity for marketing purposes. These systems will create a truly cybernetic cycle of production and consumption; because every consumptive activity will generate information pertinent to the modification of future production.'

It is through the expansion of these databases that the subject or the individual becomes increasingly 'present' as a pattern. The pattern takes the form of a dispersed and also invisible/immaterial collection of digital records stored in geographically distant places but available via the network in any place at any time for those who have the right of access.

Thus, the computer and its databases arrange information in rigidly defined categories. In relation to relatively un-contentious information such as a subjects name, age or address then this fixity of form is not limiting, in fact, it increases the speed and efficiency of many important procedures. However, when the information becomes more contentious then the reduction of this information to an unambiguous yes or no or perhaps a value on a scale of 1 to 5 then the system fixes something which, outside of the database, is extremely difficult to limit or quantify. The structure or the grammar of the database creates relationships between pieces of information, which do not exist outside of the database. But it is not difficult to imagine how these relationships may produce effects outside of the database. This means that by turning individuals into patterns determined by information entered into database fields databases or archives, these individuals become constituted by manipulating the relationships between bits of information.

No longer a "panoptic mechanism of surveillance" nor a "perspectival truth" exist according to Baudrillard, but instead of that "of a computer card that

retains your preferences" and manipulates and controls those combinations. Baudrillard suggests that we are all data, we are the models, and we are the real that is confused with the model, as in statistical operation or with the medium. He declares “the end of the panopticon”. The whole world of causality is in reservation, because if indeed everything is dependent on a model, on a simulation, then things can be overturned and recreated and manipulated and falsified without any rational link between cause and effect. The truth is simulated and we cannot be sure about the difference anymore. Whether if the claim of Baudrillard can be approved or not we can transfer to Super panoptic view of Mark Posters. When we talk about the end of panopticon Super Panopticon conceptualization becomes relevant.

What is more individuals willingly participate in the self-constitution as subjects of the normalizing gaze of, what Poster (1996), calls the 'Superpanopticon', or the network of databases which hold all of this 'personal' information. These databases and networks are not seen as an invasion of privacy or a threat to our individuality, they are seen as benign and the multiplication, and dispersal of the 'patterned' individual, which they create, is not seen to have any effect on the 'real' and present one.

Moreover to describe the subject in the age of electronic communication Poster (1996) says, '...it is multiplied by databases, dispersed by computer messaging and conferencing, decontextualised and reidentified by TV ads, dissolved and materialized continuously in the electronic transmission of symbols. The body then is no longer an effective limit of the subject's position. If I can speak directly or by electronic mail to a friend in Paris while sitting in California, if I can witness political and cultural events as they occur across the globe without leaving my home, if a database at a remote location contains my profile and informs government agencies which make decisions that affect my life without

any knowledge on my part of these events, if I can shop in my home by using my TV or computer, then where am I and who am I? In these circumstances, I cannot consider myself centered in my rational, autonomous subjectivity or bordered by a defined ego, but I am disrupted, subverted and dispersed across social space.'

Computers caused high volumes of data processing that computer industry is facing its own information overloaded. People are unable to get relevant information from computerized data. Databases' capacities are growing faster than their reorganization for information, so that an information delay exists.

The organization of data into information and information into knowledge can reduce the volume of the facts we are confronted with. We are in the age of data explosion that turns into disinformacy. It is impossible to interpret overloaded databases sources. Human are not as fast, at integrating of data into meaningful information as computers storing and processing of data. The fragmentation of consciousness because of that being slower than the improvements in technology affects the ordinary people level of awareness lack.

4.1.5 ID Cards and Mernis Project in Turkey

The digital persona of today is recorded and tracked by identification cards with numbers as barcodes on them. A step in creating digital persona -citizens in cyberspace- is to give unique numbers to each of them that can identify their personality in files as data. There are different kinds of databases and interactions between these databases resulting in personal profilings of the mass. To stabilize the order and control the ongoing procedures of state, recording and tracking of the data about individuals in society have always been crucial. Combinging new

technologies such as biometrics with an enormously powerful database, national ID Cards would become an overarching means of facilitating the tracking and surveillance. These synergy between technologies will result in unethical problems especially on ID Cards human right s can be violated.

"Surveillance technology defined as devices or systems that can monitor, track and assess the movement of individuals, their property and other assets".[32] Before these technologies were used to monitor suspects or criminals but today huge amount of haphazardly tracked, recorded mass data turns all of us to usual suspects. Here we are going to give the ID number of an ordinary Turkish citizen have to take. MERNİS is a project through which we can be a data of the profiling processes. All of our records can be matched over that specific unique number. The central population administration system in Turkey is called as "MERNİS," which is established as a database of the population to record and track the citizens in the country.[33]

An ordinary Turkish citizen has at least 24 numbers in state institutions, which are used to identify him throughout his life time (ID card, driving licence, passport, title deed, military service, weapon license, previous conviction, traffic file, OSYM (Student Selection Location Center) number, tax records, SSK (Social Insurance Organization), school, subscription of electricity, water, natural gas, commercial records, real estate taxes, bank accounts...etc.) Mernis, the central population administration system, executed by the Ministry of Internal Affairs Directorate General of Population and Citizenship Affairs, is a project to transfer all numbers to one unique number, which was given to citizens for the execution of official processes in various state institutions. This is a project to establish an integrated database - covering all the data in different databases-, which can be

[32] http://www.europarl.eu.int/stoa/publi/166499/execsum_en.htm
[33] http://www.digitaldevlet.com/haber_guncel1.php.htm

investigated with this unique number. With the help of this new number called Mernis no. Which has 11 digits, the main aim is to be able to see all data related to a citizen on the computers when making an investigation in one state institution. It is the target of this project that approximately 120 million Turkish citizens, including the missing and deceased, will be numbered.

The project was put into practice on Sept. 1, 1974 with the Population Law no. 1587. The State Planning Organization developed the project in 1976. METU (Middle East Technical University) won the related tender in 1980. The project implementation studies began in 1982. The World Bank included the Mernis project into its agenda of privatization and social security network in 1996. The Bank transfers its resources to the project and a project management support agreement was signed with the United Nations Development Program. The budget of the project is foreseen as 100 million dollars. The distribution of identification numbers began in 2000. It was reported that smart cards that cannot be copied would be distributed as a next step of the project. The criticism towards the project is as follows: There is a possibility that these data which are gathered in one database might be seized by unauthorized parties other than the citizen himself and the relevant state institution. In your daily routine you can observe after you ara recorded for some official purposes later on they will easily recall your personal settings. These data are used for matching and profiling the masses. Your ID number can turn into a spy inside you, and will alert the authorities if you did not pay your bills, or you did not attend your military obligation, or you can not take a credit because of your not paid bills in the past. Even worse than that our DNA will talk about us as an inside enemy if the power holders will succeed in application of ID with fingerprint projects. This is not a conspiracy theory if we closely observe the developments in new technologies.

4.2 Alternative Attitudes towards Supervision/ Coercion of New Technologies Impact of the Information Age on Terrorism/ Hacktivism

In common agreement at discursive level, cyberterrorism equaled with hacking, but at the beginning hacking had an ethical bias. Today the limits of each blurred. We believe that if the goal is to gain power of knowledge without discrimination between any of us, it is a way of resistance, civil disobedience but if the attacks hurt living creatures then we have to talk about terrorism. As a way of activism artistic political resistance in age of information, we support the main ideal passed through the first hackers in MIT (Capurro , 2003).[34]

Despite the fact that the political, cultural and social motives behind acts of terrorism remain the same in the information age, recent developments in information and communication technologies have brought about significant and complicated changes with regard to international terrorism. The most important development that the information age brings about regarding the issue of terrorism is that highly advanced technological opportunities have become available not only for ordinary citizens but also for terrorists.

The emergence of a new type of terrorism along with the information age indicates that the acts of terrorism have undergone a significant, organizational, strategic and technological transformation. One of the most important results of the information revolution is the rise of organizational structure in the shape of networks both in national and international arenas.

[34] http://www.capurro.de/illinois.html

Therefore, the more the networked organizational structures spread, the more international the terrorism becomes. At the same time, terrorists have obtained to opportunity to hide themselves and their illegal activities in cyberspace. In addition, terrorists are today able to destroy information databases and backgrounds of their targets besides organizing physical attacks. Should the terrorists adopt a new strategic method based on swarming rather than organizing individual attacks, it would become more and more difficult to fight them in national and international arenas. Since terrorist groups have become more flexible and less hierarchic organizations in addition to their ever-increasing usage of advanced technologies for commanding, monitoring and coordinating their activities, even relatively small terrorist organizations have become the actors of worldwide illegal acts. Advanced information and communication technologies have offered terrorists new dimensions, and provided them with limitless opportunities for better communication. Among the potential targets of the terrorists using these technologies are information databases, information processing structures and communication systems. The more dependent the modern nation state becomes upon computer-based information and communication technologies, the more fragile it becomes to terrorist attacks.

Today, there is a potential for terrorist organizations to benefit from these new technologies to attack information systems, taking less risks when compared to past. While the financial cost of acts of terrorism decreases with these technologies, terrorists are very likely to become more willing to use them in the future as their possible destructive impacts and accessibility increases. Laqueur (1996) remarked as follows on this dimension: “If the new terrorism directs its energies toward information warfare, its destructive power will be exponentially greater than any it wielded in the past -- greater even than it would be with biological and chemical weapons”.

These technologies have made activities of communication and network possible. In addition, cyberspace provides people with hidden communication channels and the opportunity to hold anonymous activities. It is known that terrorist organizations have engaged in exchange of information and cooperate with other terrorists in cyberspace. As such communication is the potential target of the national security and intelligence agencies, these groups have chosen to use encrypted codes.

The inexpensive nature of Internet made it popular among the terrorist groups. As the computers become smaller, more inexpensive and more user-friendly, cyberspace becomes more available and convenient for acts of crime and terrorism. Communication technology lessens the importance of distance. One of the reasons why terrorists prefer to use information technologies is that since they are rejected by mass media, they get the opportunity to reach their target groups via these technologies, especially young and educated ones.

The content of information can be classified under three titles which sometimes coincide with each other: First, military information, including general military activities, secret operations, intelligence activities etc. Second, business information, including business records, banking processes and other financial processes. Third, personal information, including personal records, personal systems and files etc…

Since the info-war is an electronic conflict where information is considered a strategic tool which worth to be captured or destroyed, computers

and other information systems have become prior targets for terrorists. An information war campaign might cause great damages on important civilian, commercial and military systems such as air traffic control, stock markets, and international commercial activities. A possible attack on compiled military information in fact poses a great national threat.

In every war science and technology are used, and the more the scientific capacity increases, the more advanced the weapons used in wars. There are three basic reasons behind the increase of electronic terrorist attacks in the recent years: First, the usages of Internet in such attacks have globally increased along with the number of potential assaults and targets. The second reason is the existence of approximately 30.000 hacker web sites that have made their capability to organize digital attacks public. The last reason is that terrorist groups themselves have become multidimensional leaving behind old world's limitations and ideologies in the wake of the Cold War. Due to these new political realities combined with available cyber weapons, the threat posed by terrorist groups has considerably increased.

The reason why the issue of cyber terrorism is becoming more serious day by day is the lack of information in public and private sectors on how fragile they become to cyber attacks. Recent studies have shown that critical infrastructures can easily be damaged by cyber terrorist attacks. Although it is possible to remove most of the weaknesses in computer systems, it is impossible to eliminate all of them. However, the critical infrastructures are often fragile against cyber terrorist attacks, there are not much actors who have the motivation and capacity to organize such illegal operations. In other words, although most of the hackers have enough information, skills and tools to attack to computer systems, they do not have sufficient motivation to hold serious attacks, which would cause great

economic and social damages. These people require certain tools and the ability to use these tools in order to organize massive destructive acts.

> The hackers transformed computers and the Net into a social medium that was not part of either the governmental or corporate plans. Email was invented in July 1970 by Ray Tomlinson, who is also the one to thank (or blame) for the @-symbol in email addresses. Abbate describes the consequence of this unexpected innovation: "ARPANET users came to rely on email in their day-to-day activities, and before long email had eclipsed all other network applications in volume of traffic." From then on, e-mail has been the most popular use of the Net (Himanen, 2003 cited in Capurro).[35]

Internet provides people with an important space for their propaganda and psychological war, furthermore terrorists use laptops. Amateur hackers who are only curious about discovering information systems for their own interests rather than organizing politically violent acts might become professionals under the management of an employer. These employers are not only non-state terrorist groups but also the states themselves that employ these hackers for their country's national interests.

Hackers might crack passwords, steal files, download destructive programs on specified targets or organize attacks preventing public services. Hackers might feel themselves powerful due to great media attention or their ability to hack state computer however, this does not mean that governments would be forced to change their stances on national security and foreign policy issues.

Another destructive type of cyber activity is misinformation. Thousands of Internet users in the world are able to express whatever they wish without any fear

[35] http://www.capurro.de/illinois.htm

of state intervention or punishment. Because of the misinformation, people might suffer in great fear and paranoia. The US Monterey Navigation Graduate School Terrorism and Disorganized War Studies Center prepared a report to put forward the possibility for the terrorist organizations which attempt to organize cyber attacks to realize their goals: The report entitled 'Cyber Terrorism: Possibilities and Signs' states that terrorist groups are unable to organize massive or global cyber terrorism organizations in terms of their tools and human resources (Benner, 2001).[36]

The report defines three cyber terrorism capacity levels:

The first level is the basic level, which indicates the capacity to hold simple hacking activities that would damage personal system by using tools created by others. An organization at this level has a low level of target analysis, command control and learning capacity. The second level is the advanced level. Organizations at this level can organize more complex attacks towards multidimensional systems or networks. These groups have basic level of target analysis, command control and learning capacity. The last one is sophisticated level, which means that such organizations are able to organize coordinated attacks against integrated and heterogeneous defense systems resulting in great damages. These groups have high level of target analysis, command control and learning capacity.

There are two methods through which terrorists organize cyber terrorism attacks in the information age. In the first one, information technology itself is the

[36] http//www.salon.com/tech/feature/2001/04/04/cyberterrorism/index..htm

target, and in the second one, information technology is the tool of a larger operation. In the first method, terrorist is the saboteur of the information system, damaging the system itself or other information infrastructure dependent on the targeted system. In the second one, terrorist organization uses the information system to change or steal data. They manipulate the system for an undesired or unplanned function.

4.2.1 Transgression into Systems: Hacking

Transgression to systems known as hacking creates different security problems. Hacking might occur in different ways. Systems are exposed to attacks for gathering or stealing information or an atmosphere of panic and fear is created via downloading systems incorrect information.

All viruses, Trojan horses and worms have great destructive powers. Viruses are computer programs, which are able to attach to computer files, immediately copy themselves and spread like an epidemic as the infected files are downloaded to different computers. The more a computer engages in activities with others, the higher its possibility to become infected with viruses. Trojan horse is a system seems innocent but after get into your computer it starts to be effective as the name it borrowed from historical story of Troja.

The difference between semantic attacks and hacking is that hacking causes random or systematic problems in systems and causes them to be out of order immediately after the attack. However, the system, which is exposed to a semantic attack, seems to continue processing as if it functions correctly.

Information revolution has caused rooted changes in the definitions of the possible conflicts that the societies might deal with and how security forces should prepare and respond to these conflicts. The Network War, in general terms, is a newly emerging type of conflict where non-state actors such as terrorist groups use networked organizations, doctrines strategies and technologies. Very significant transformations are taking place in the organizational structures of international terrorist groups, their conducts of behavior and the threats posed by them. National and international security problems of the information age are much more disorganized, multidimensional and ambiguous.

Human factor always causes unintended consequences different then predictions of power holders whether or not they record, categorize, and track human beings by digitalization. There is always a way to escape the system at its blind spots. So that hacktivism can be a way to resistance in relation with other types of movements and actions.

CHAPTER 5

CONCLUSION

The substantial application of the technologies of personal and mass surveillance has been experienced throughout the last century. The next decades may see technologies of identification, location and tracking destroying the individuals' freedom. Counter attacks to those tendencies are new forms of networking that have been enabled by the Internet. These have created the possibility of intensified freedom and power for individuals and social groups. Government authorities and corporations, however, are implementing substantial counter improvements. This is designed to overcome the potential for net-based freedoms and to guarantee the maintenance and improvement of social control.

Why are we today inclined to attach more significance to recording, tracking and monitoring activities of power holders (e.g.states and multinational corporations)? Because, during the last decades social awareness has become more difficult to be achieved. States and other power holders by means of various technological tools do manipulate accepted common rhetoric. New technologies have significantly helped states and MNCs to establish much more sophisticated and complicated monitoring and surveillance mechanisms. When compared to the past, the mechanisms of surveillance have become much more embedded and diffused in our lives, and made it almost impossible for individuals to become aware of the fact that they are being watched. Individuals are not aware that their personal information is being collected and compiled in various databases. In

other words, citizens do not know that even themselves are turning into nothing but an accumulation of data for their states. It is very difficult to fight such a complicated system by using classical opposition methods even though if people are aware of this fact.

Modern surveillance, which emerged due to certain institutions such as the army, the state and private corporations, has become so much embedded in every aspect of our lives that it has made itself almost invisible. In the past, alienation referred to blue-collar workers' relation with their jobs and their fight with a sense of estrangement when they saw another worker, whom they were working side by side in an assembly line, losing his arms in a job accident. It was relatively easier for them to comprehend how alienated they were from both their jobs and other workers, or maybe the life itself. However, today, white-collar workers, who are totally separated from each other in their more hygienic and isolated offices and with their totally personalized computers (in other words, in their personal ghettos) are alienated from the concept of alienation itself. That is to say, this is nothing but a meta-alienation process that people are undergoing as a critical experience, which is why it is more difficult to be aware, and more difficult to feel the necessity for awareness, and to fight against the above mentioned data-gathering process as a part of a more sophisticated surveillance system.

Therefore, the modern – or postmodern, to say it in a more fashionable style – individual is day-by-day going far away from the integrity of information and a holistic understanding of the world he lives. He or she is more incapable of understanding the ongoing scenario. The more fragmented life becomes, the less we understand it. Individuals are losing their opportunity to get organized as they are equipped with much more fragmented information thanks to individual consumption services and specialization, which should be considered as "alienation effects" of our lives. We are only experiencing a sense of refraction

when we encounter serious problems with the system itself. That is to say, whenever we stop acting like good citizens, we hit the invisible walls of the system and see how confined we are in a huge *superpanoptic* prison (Poster, 1996).

What we call "alienation to alienation" refers to a mode of perception where people are not capable of understanding that they are touching an elephant while they are touching its body parts. Individuals have lost the power of imagination of a whole as its parts are much more fragmented. Our daily routines are so much dependent upon our credit cards, MERNİS (in Turkey) numbers, SSN (in America), e-mail addresses and cell phones that we cannot even imagine to survive without them.

Rapidly developing technological innovations are continuously increasing this capacity of surveillance by producing cheaper, easily accessible and more user friendly tools (chips, mobile phones synchronized with Global Positioning Systems, Facial recognition systems, biometric gadgets).

It is like a nightmare, which is making it more difficult to wake up. The will and the desire to wake up means "awareness." In this age, where old opposition and fighting mechanisms are eliminated and absorbed by the system, the first step towards "a phase of awareness" is to realize what goes on around us and to understand the rules of the game. It is not possible for us to completely deny the benefits of new technologies or to turn a blind eye to its effects on social structures that we are living in. What we must do is to refrain from over-exaggerating these effects, as if we are living in a technologically manipulated society.

The latest developments in ICT, as declared by military authorities caused a new type of power clashes; the new warfare is in cyberspace. The more you get the information about others the more you gain power in the cyberspace. This is the main reason why we highlight the hacktivism[37] as an alternative disobedience. Hacking with social consciousness and political activation against to coercion of power holders is necessary to survive in brave new world. However, there is a problem at the point of how could we turn all these abstract issues, which are debated in a very closed circle and only understood by a hand full of technicians, into a large topic, understood by the millions, so to speak? Minor decisions in the realm of technical standards taken today will have enormous effects on society later on.

Possessing the means of production of information results in having the ruling power. Negative attitude against electronic surveillance in general is called *resistance* in theoretical realm. If electronic surveillance can be seen as a form of discipline, the resistance to that coercion and pressure has to be built within that realm.

Disobedience is a right of every individual, which means to resist the coercion of the power holders through the hegemonic structure. There is a hope in information age. The individual can use the same instruments with power holders; the only way to posses the power is to have the knowledge about the instruments. The first step to have the knowledge we insist on awareness. Being aware of the other brings the realization of the weak and strong points of it, and at the same time yours. If we can be aware of the importance of new technologies surveillance capacity we can also gain the knowledge of defense and assault points, which we called blind spots of the system through out our study. According to Foucault (1988) the link between power and resistance is tight, because they produce each

[37] http://searchsecurity.techtarget.com/originalContent/0,,sid14_gci506135,00.html

other mutually. The resistance is a method of creating cleavages in the balances between subservient and master.

We can quote the famous words of Napoleon Bonaparte to show the importance of intelligence and knowledge in the warfare of our century, 'There are but two powers in the world, the sword and the mind. In the long run the sword is always beaten by the mind'. The possibility of resistance comes from the capacity of the awareness of individuals being involved in information production. If the break can be achieved within the *alienation-to-alienation* realm, the individuals can see the blurred matrix eyes wide open.

Bearing in mind that each conspiracy theory might have a connection to the reality at one point, we should also abstain from extremely optimist approaches that imagine a heaven-like future thanks to new technologies. Our suggestion is to be aware of the surveillance process, to know its rules and develop new opposition methods and new defense positions. We should not either forget that paranoia scenarios might even be useful to power holders since they nourishes the sense of there-is-nothing-to-be-done. The inseparable character of infrastructure and superstructure in the last decades makes this dominant discourse even more dominant and taken-for-granted thanks to the very structure of the system which keeps us away from awareness. From the point of social Darwinists, in the current structure of the system (which might be called as "the survival of the fittest"), some people unfortunately lack even the basic information about the rules of the game, which makes it impossible for them to reach a state of "complete awareness." Surveillance takes place in the world of invisible numbers, in a digital world, however this information is gathered from our daily lives.

People leave our electronic footprints everywhere, whenever we draw money from our bank accounts or become a member to a club or fill a form to apply to a job etc. Many services and products, which are meant to liberate us from our daily routines, are making us unwilling participants to this data collecting process as a subordinate on the contrary to the will of liberation. We ourselves become data, which can be recorded, tracked, filed and monitored. If the system implements such surveillance practices in unrestrained ways, we should then be immediately aware of its methods and develop our own. Because, technology is rapidly growing and new security laws and agreements in favor of power holders legitimize the surveillance process for the sake of increasing security, efficiency and productivity. The laws such as the Patriot Act which was developed in the wake of Sept. 11 incidents to authorize the state in intervening into databases without questioning display us how critical the current situation is. At this point, certain activities that are considered illegal such as encryption in Internet communication and hacktivism might be seen as "new defense systems." Another assumption is that hacking might be considered as "civil disobedience," or "a political counter stance", if its goal is to provide people with equal opportunity to access information and to oppose operating systems that are closed resource systems.

Freedom from our restraints, awareness about superpanoptic cage surveillance can be turn upside down and we can still be hopeful. A third way situated between paranoia and ignorance is awareness. Not only the surveillance characteristic of the information age would then be eliminated, but it would also be turned into a knowledge age by the awareness of human beings about the opportunities of technology and by learning defense techniques against privacy invasion under the supervision of power holders.

REFERENCES

Allon, Fiona in (Spacing & Timing: rethinking Globalization & Standarization Palermo, Italy 1-3rd november 2001) *An Ontology of Everyday Control: Space and Time in the Smart House*
http://www.emp.uc3m.es/~quattron/conference/papers/Allon.pdf

Bell, Daniel (1973). The coming of post-industrial society. New York: Basic Books.

Bell, D. (1979). The Cultural Contradictions of Capitalism. London: Heinemann.

Beniger, J. R. (1986). The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge: Harvard University Press.

Bentham, Jeremy (1962). The works of Jeremy Bentham (J. Bowring, ed.). New York: Russell and Russell.

Bogard,William (1996). The Simulation of Surveillance: Hypercontrol in Telematic Societies. Cambridge: Cambridge University Press.

Bozkurt, Veysel (2000). EnformasyonToplumu ve Türkiye. İstanbul: Sistem Yayıncılık.

Burgess, P. (1994) *European Borders: History of Space/Space of History*, *Ctheory,* www.ctheory.com/article/a013.html.

Campbell, D. "*Inside the Echelon"*.
http://www.heise.de/tp/english/inhalt/te/6929/1.html

Carey, J. W. (1989). Communication as culture: Essays on media and society. Boston: Unwin Hyman.
http://www.wlu.ca/wwwblack/cS400/fall02/October8.html

Capurro, R. (2003). "*Passions of the Internet and Art of Living"*.
http://www.capurro.de/illinois.htm

Castells, Manuel (1996). The Rise of the Network Society. Oxford: Blackwell.

Castells, M. (2000) The Rise of the Network Society (2nd edition). Malden: Mass., Blackwell.

Clarke, Roger A. (1988). *Information Technology and Dataveillance*
http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html

Clarke, Roger (1994). *The Digital Persona and its Application to Data surveillance*
http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html

Cox, R.W. (1996). Social forces, states and world orders: Beyond international relations theory. In R.W. Cox with T. J. Sinclair (Eds.), *Approaches to world order* (85-123). Cambridge: Cambridge University Press.

Davies, Simon (1992). *Big brother: Australia's growing web of surveillance,* Sydney: Simon & Schuster.
http://www.pco.org.hk/english/infocentre/files/davies-paper.doc

Dertouzos, M. L. (1991, Sept.). *Communications, computers and networks*. Scientific American, 4, 62-69.

Dillion, John (1997) *The Internet is changing from a Public resource to a Lucrative Operation influenced by Spooks and former Pentagon Officials. Open access and Information are increasingly controlled.*
http://mediafilter.org/caq/internic

Dordick, H. S., & Wang, G. (1993). The information society: A retrospective view. Newbury Park: CA: Sage.

Drucker, Peter. (1993). Post-industrial society. Butterworth: Heinemann.

Druckrey, T. "*Strategizing Against Inevitability*," in: A*bsolute One – Catalogue of the Slovenian Pavilion at the 49th Venice Biennial*, Venice 2001 at http://absoluteone.ljudmila.org

Ellul, J. (1964) The Technological Society. New York: Vintage.

Escobar, A.(1994). Welcome to Cyberia: notes on the anthropology of cyberculture.
Current Anthropology 35: 211-231.

Foucault, Michel (1977). Discipline and Punish: The Birth of The Prison. London: Penguin.

Foucault, M. (1980) in C. Gordon (ed.) Power/Knowledge: Selected Interviews and Other Writings. Pantheon Books.

Foucault, M. (1982). "*The Subject and Power*", *Critical Inquiry, 8*, 777-795

Foucault, M. (1988). The ethic of care for the self as practice of freedom. In: Bernauer, J.and Rasmussen,D. (eds.)The Final Foucault. Cambridge, MA: MIT Press.

Gandy, Oscar. (1993). The Panoptic Sort: A Political Economy of Personal Information Colorado: Westview Press.

Gandy, O. H. (1996). 'Coming to Terms with the Panoptic Sort'. *Computers, Surveillance, and Privacy*.
http://www.asc.upenn.edu/usr/ogandy/IAMCRdatamining.pdf

Garfinkel, Simson, January 2001, "*Database Nation The Death of Privacy in the 21st Century"*.
http://www.oreilly.com/catalog/dbnationtp/chapter/cho3/ch06/ch09.html

Gibson, William (1984). Neucromancer. New York: Ace Publishing Company.

Giddens, A. (1985). Social Theory and Modern Sociology. Cambridge: Polity Press.

Gill, S. (1995). Globalisation, market civilisation, and disciplinary neoliberalism. *Millennium: Journal of International Studies, 24* (3), 399-423.

Goffman, (1961). *Asylums: Essays on the Social Situation Mental Patients and other Inmates.* Harman and Sword: Penguin

Gouldner, A. (1979). *The future of intellectuals and the rise of the new class: a frame of reference, theses, conjectures, arguments, and an historical perspective on the role of intellectuals and intelligentsia in the international class contest of the modern era*. London: Macmillan Press.

Hauben, R. (1997**)** The Birth and Development of the ARPANET

Haywood,T. (1995). Info-rich –info-poor: Access and exchange in the global information society, New Jersey: Bawkur- Saur Publishing.

Held, D. (1998). Democracy and Globalization. In D. Archibugi, D.Held & M. Köhler (Eds.), *Re-imagining Political Community* (11-27), Polity Press.

Hiltz, S. R., & Turoff, M. (1978). The network nation: Human communication via computer. Reading: Addison-Wesley.

Hirschheim, R.A(1991). "*Information systems epistemology: A historical perspective"in* Galliers,R.(eds.)Information Systems Research:Issues, Methods and Practical Guidelines, 28-60.

Huntington, S.(1993) The Clash of the Civilizations
http://www.lander.edu/atannenbaum/Tannenbaum%20courses%20folder/POLS%20103%20World%20Politics/103_huntington_clash_of_civilizations_full_text.htm

Kevin Robins and Frank Webster, *Times of Technoculture: From the Information Society to the Virtual Life*. New York: Routledge, 1999.

Kitchin, Rob (1998) Cyberspace*:* The World in Wires, New York: John Wiley & Sons Ltd.
Komiega, Kevin(2000) Political hacking: Crime or activism?
http://searchsecurity.techtarget.com/originalContent/0,,sid14_gci506135,00.html

Lauda D.P., Ryan R.D (1971)(edi.) Advancing Technologies: Its impact on society, USA WM.C.Brown Company Publishers

Laquer, Walter "*Postmodern Terrorism: New Rules for an Old Game*", *Foreign Affairs*, Vol.75, No.5, September-October 1996, pp.24-36

Lynch, Daniel C. (1993). Historical Evolution. In *Internet System Handbook*. Daniel C. Lynch and Marshall T. Rose, eds. Massachusetts: Addison- Wesley Company, Reading.

Lyon, David (1988) The Information Society: issues and illusions, Cambridge, Polity Press.

Lyon, D. (1993) "*An Electronic Panopticon? A sociological critiques of surveillance theory", The Sociological Review, 653-678.*

Lyon, David (1994) The Electronic Eye: The rise of surveillance society, Minneapolis: University of Minnesota Press.

Lyon, David and Elia Zureik (ed.) (1996) Computers, surveillance, and privacy, Minneapolis, University of Minnesota Press.

Lyon, David (2001) Surveillance society: monitoring everyday life, Phildelphia: Pa., Open University.

Machlup, F. & Mansfield, U. (Eds.). (1983). The study of information: Interdisciplinary messages. New York: John Wiley & Sons.

Marx, G.T. (1988) Undercover*: Police Surveillance in America.* Berkeley:CA:

Marx, G.T. (1996) *'Electric Eye in the Sky: Some Reflections on the New Surveillance and Popular Culture' Computers, Surveillance, and Privacy*.

McLuhan, M. (1964). Understanding Media: The Extensions of the Man. New York: Macmillan.

McGarty, T.P., and Haywood, C. (1995). Internet Architecture and Policy Implications for Migration from High-End user to the New User. In B. Kahin & J. Keller (Eds.), *Public Access to the Internet: A Publication of the Harvard Information Infrastructure Project* Cambridge: MIT Press**.**

Naisbitt, J. (1982). Megatrends: Ten new directions transforming our lives. New York: Warner Books.

Negroponte, N. (1995). Being Digital.New York: Vintage Books.

Orwell, George(1965) Nineteen eighty-four. Harmondsworth :Penguin.

Perolle,J.A,(1996,1997,1998). Computers and Social Change. Word Sworth Publishing Company
e-book :www.ccs.neu.edu/home/perrolle/book/Word Sworth Publishing company new material 96/97/98

Poster, M. (1996). *'Databases as Discourse; or, Electronic Interpellations'***.** Computers, Surveillance, and Privacy in Lyon, D. and Zureik, E. (ed.) Minneapolis, University of Minnesota Press: 175-192.

Poster, M. (1995). The Second Media Age. Oxford: Polity Press.

Rainbow, Paul (1984), The Foucault Reader. New York: Pantheon Books.

Reinecke, Ian (1984). *Electronic Illusions: A Skeptics View of Our High-Tech Future***.** New York: Penguin.

Robins, K., & Webster, F. (1988). Cybernetic capitalism: Information, technology, and everyday life. In V. Mosco & J. Wasko (Eds.), *The political economy of information* (pp. 44-75). Madison: WI: University of Wisconsin Press.

Rosenbrock, H. H. (1990), *Machines with a Purpose*, OUP.

Rosenau, J.N. (1995). Governance in the Twenty-First Century. *Global Governance, 1,* 13-43.

Roszak, Theodore (1994). The Cult of Information: The folklore of computers and the true art of thinking. Berkeley, CA: University of California Press.

Sarup, M. (1993). Post-structuralism and Postmodernism. Athens: University of Georgia.

Scholte, J.A. (2000). *Globalization; A Critical Introduction*. New York: St. Martin's Press.

Sullivan, B. (2001). FBI confirms 'Magic Lantern' exists, Dec. 12, 2001. http://www.msnbc.com/news/671981.html

Sutherland, E. *The Information Society*.
http://www.lamp.ac.uk/ewan, http://sutherla.tripod.com/infsoc/inf_rev/

Toffler, A. (1981). The Third Wave, New York: Bantam Books.

Üney, Tuncer (2000). TBV Report, Kamu Uygulamalarına Farklı Bir Bakış.
info@tbv.org.tr

Veysel, B. (2000*).* Enformasyon toplumu ve Türkiye. Ankara: Sistem Yayınları.

Virilio, P., Rose, J.(1994). The Vision Machine Indianapolis: Indiana University Press.

Weizenbaum, Joseph (1976). Computer Power and Human Reason: from judgement to calculation. San Francisco: Freeman Publishing.

Winner, Langdon (1992). Virtual Office Electronic Prison excerpt from "Silicon Valley Mystery House". In Variations on a Theme Park: The New American City and end of Public Space. Micheal Sorkin (eds.) New York: Noonday Press,

Wright,S. (1998). 'An Appraisal of Technologies of Political Control', European Parliament, Scientific and technological Options Assessments working document. Luxembourg: European Parliament, Director General for Research, Directorate B, the STOA Programme.

Zey, M. (1984 The Mentor Connection Homewood. IL:DownJones- Irwin.